Council of the European Union

Brussels, 1 December 2017
(OR. en)

15174/17

LIMITE

DAPIX 411
COMIX 815
JAI 1153
FRONT 496
ASIM 134
COPEN 393
ENFOPOL 596
SIRIS 210
VISA 446
SCHENGEN 84
CT 154

NOTE

From:	Frontex
To:	Delegations
Subject:	Non-paper by Frontex on its access to central EU systems for borders and security

Delegations will find enclosed the above-mentioned paper, submitted by Frontex, in view of the upcoming legistative proposal on interoperability.

Warsaw, 16 October 2017

Frontex Non-paper

Subject: Frontex access to Central EU Systems for Borders and Security

1. Introduction and aim

Through this non-paper, the European Border and Coast Guard Agency (Frontex) would like to contribute to the discussion in the Council Working Party on Information Exchange and Data Protection (DAPIX) on access to central EU systems for borders and security. This non-paper is also intended to support the Commission's preparatory work regarding the upcoming legislative proposal on the interoperability of information systems for migration and security[1].

In this non-paper, Frontex has partially included the table in which the Commission and the Presidency mapped the various central EU systems and the different purposes for accessing them[2] (see Part 3 below). This table generally reflects two types of access for Frontex: (1) access by European Border and Coast Guard Teams (EBCGT) and teams of staff involved in return-related tasks as well as by Migration Management Support Teams (MMST), (hereinafter "members of the Agency's teams"), including to personal data, and (2) access by the Agency to certain statistical data.

As the table depicts, the Agency's access to these EU databases is more restricted compared to the access by other competent national authorities. This is an important discrepancy given that the members of the Agency's teams have to implement executive missions (e.g. border control or identification and registration as part of migration management or return tasks) under the jurisdiction of the competent national authority where the operation is taking place. This restricted, or even lack of, access negatively affects the operational support that the Agency can offer to the Member States.

Therefore, Frontex proposes that the Commission addresses this discrepancy in the interoperability package ('Omnibus') by: (1) taking into account the need **to align the access rights of the members of the Agency's teams with those of the national authorities performing equivalent tasks**, and (2) supporting Frontex in undertaking risk analysis, vulnerability assessments and providing the situational picture **by improving the Agency's access to statistical data from these EU systems**.

In the following non-paper, both legal and operational arguments are put forward in favour of this approach.

2. A case for enhanced operational access to central EU systems

The creation of the European Border and Coast Guard serves a well-defined Union goal. According to Recital 2 of the European Border and Coast Guard Regulation (hereinafter 'the Regulation') this goal is to ensure the security of the Union's external borders by implementing and developing IBM.

One of the key enabling factors of IBM is the concept of ***shared responsibility*** laid down in Article 5 of the Regulation and elaborated on in Recital 6. The Agency is bound to implement IBM as a *shared responsibility* of Frontex and of the national authorities performing border control, including coast guards.

While the implementation of IBM entails varying reliance on certain components over others, **the use of state-of-the-art technology, including large-scale IT systems, is key** in the context of the Agency's operational

[1] *Inception Impact Assessment, Interoperability of information systems for migration and security, Ref. Ares (2017)3765711 - 26.7.2017.*

[2] *Council of the European Union, Access to central EU systems for borders and security, 12258/17, 20.9.2017.*

activities and other services provided to the Member States in accordance with the Regulation. Recent policy developments related to border security and asylum only serve to prove this point.

Therefore, ensuring the fullest access to EU systems **facilitates the Agency's *shared responsibility* of implementing IBM at the external borders.** Stipulating this explicitly in the IT systems' founding Regulations or including it in the upcoming interoperability package **does not entail an expansion of the Agency's tasks.** To the contrary, this ability to access these systems (for personal and depersonalised data) is envisaged by the Regulation, and is the very essence of a fully functioning obligation to ensure the security of the Union's external borders *collectively*. At the same time, this ability would enable Frontex, in cooperation with eu-LISA, to make use of **interoperable, secure and uniform access interfaces such as the European Search Portal, developed as a follow-up to the recommendations of the High Level Expert Group.** In this context, the interoperability package would be a good possibility to enhance the accountability and transparency of the Agency's access to central EU systems through full compliance with these systems' legal frameworks and the applicable data protection regime.

Finally, it should be underlined that EU legislation should refer to the use of Frontex's own interface and ICT equipment for access to, or even transmission of, data as a ***possibility***. Inserting this as a *possibility* in EU legislation will give Frontex much needed flexibility. This is so because Frontex must always assess beforehand the Member States' concrete requirements for increased technical and operational assistance, and **agree with the Member State hosting the operation on the need and modalities for the use of its own ICT equipment** which would allow the Agency's team members to connect to central EU systems.

Leaving the matter of access to central EU systems aside, the Agency's capacity to implement IBM would be enhanced even more through access to Interpol databases. However, this will be approached through separate legal and institutional avenues given that the future interoperability package may not tackle this issue. Distinct procedural steps will need to be undertaken.

2.1 Access by members of the Agency's teams in the context of Frontex operational activities

2.1.1 Purpose of access: Border control performed by EBCGT

IBM calls for aligning access rights especially in joint operations where EBCGT have not only supportive but also executive roles under the supervision of the host Member State.

Providing for the possibility of access in the founding Regulations of large-scale IT systems would guarantee consistency with Article 40(8) of the Regulation. This provision already envisages the obligation for host Member States to authorise members of the teams to consult European databases. The rationale for such access is simple. If national authorities have or should have certain access rights in performing border control, the Agency's EBCGT should have equivalent access when performing the same task in the context of an operation. This is indispensable for the Agency's team members to be fully functional when deployed at the external borders, and to help national authorities cope with large flows of migrants or travellers at border control points (BCPs).

This type of equivalent access will require a technical solution which would allow the team members to be able to access the same information that is available to the competent national authority. At the implementation phase, we will need to consider how to address the need to search national databases apart from central EU systems. In any case, the added value for Frontex of deploying its own ICT equipment for the team members is related to the possibility to make additional information systems available which are currently not accessible to national authorities when performing border control.

2.1.2 Purpose of access: Migration management performed by MMST

Pursuant to Article 18(4) of the Regulation, MMST are tasked to provide assistance in screening third-country nationals (TCN) arriving at the external borders (including the identification, registration, debriefing, and where requested by the MS, fingerprinting).

In order to provide effective technical and operational assistance in support of the 'hotspot' approach in cooperation with EASO and Europol, Frontex requires the possibility for a similar type of access to EU databases as competent national authorities performing the same tasks. **As mentioned above, such access is not an**

expansion of the Agency's mandate since it is already provided for in Article 40(8) of the Regulation for EBCGT and return-related staff (who are part of MMST).

The most efficient way for the agencies to assist with registration is to have their own equipment and own interface for the team members. Frontex could reinforce ICT capacities at hotspots with wireless routers, laptops, fingerprint readers or cameras. The personnel deployed would need access for the purpose of migration management to the various EU systems in the way mentioned in the table included in part 3. This could also be an excellent operational scenario for testing the European Search Portal, capable of searching in parallel all relevant EU systems in the areas of borders, security and asylum.

2.1.3 Purpose of access: Return of irregular Third Country Nationals (TCN) performed by teams of staff involved in return-related activities

The Agency is mandated to provide technical and operational assistance for Member States in the field of return, namely coordinating the use of relevant IT-systems, according to Article 27(1)(c) of the Regulation.

Therefore, in a similar way to the operational activities described above, aligning the access rights for the Agency's return specialists in return related activities (such as in pre-return activities and identification of TCN and in the context of return interventions[3]) to the one of the competent national authorities is required. As interoperability between EU systems increases, the support they can provide to return practitioners, in particular for an accurate identification of TCN in view of issuing a return decision or travel documentation, will also significantly increase. **Once again, such enhanced access by the Agency is already mandated and provided for in Article 40(8) of the Regulation.**

Furthermore, the Commission should seize this opportunity to create, confirm or clarify the access rights to these EU systems by the national authorities for the purpose of return. Clear legal provisions would support **further harmonization of national return practices regarding the use of EU large scale IT-systems for identification and documentation purposes.** Such provisions would also facilitate the work and operational support to the Member States by the Agency's teams involved in return related tasks.

2.2 Access to depersonalised data in EU large-scale IT systems for risk analysis, vulnerability assessments and for providing the EU situational picture

At the same time, the use of depersonalised data retrieved from EU systems could be one very important stream of information **for the Agency's information products which include risk analysis and vulnerability assessments is accordance with the Regulation, and the situational picture in accordance with the EUROSUR Regulation[4].** Risk analysis, vulnerability assessments, early warnings for visa liberalisation monitoring[5] or risk analyses related to reinstating targeted checks pursuant to Article 8(2b) second subparagraph of the Schengen Borders Code[6], could be substantially enriched with these statistical data, including those generated through their use by the Member States such as searches and hits.

Furthermore, the statistical data generated through the use of EU systems can also support the development of a more complete situational picture of the EU external borders which falls within the remit of EUROSUR.

However, the current legislation does not take fully into account the diversity of these tasks. For these statistical purposes, Frontex does not currently have access to statistical data from certain databases (notably VIS), while Eurodac and SIS II are currently still under discussion.

It should be stressed that the analytical products or situational picture are being developed for the benefit of the competent national authorities as well as EU Policy Makers for an even better informed and evidence-based policy decision making.

From the Agency's point of view, the use of these type of statistical or metadata should be acknowledged and promoted. Given that the direct processing of personal data is not a concern in this context, the relevant legal provisions should not unnecessarily restrict the use of statistical data only to certain articles of the Regulation

---

[3] See Article 33 of the Regulation.

[4] Regulation (EU) 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR), (OJ L 295, 6.11.2013, p. 11).

[5] Especially Article 29 of Regulation (EU) 2016/399 of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), (OJ L 77, 23.3.2016, p. 1).

[6] Ibid.

(as it is the case with the Commission's proposals or the latest amendments to EURODAC, SIS II or EES Regulation (agreed)). It would be more sensible to refer generally to the purpose of implementing the Agency's mandate and in particular to risk analysis, vulnerability assessments and for the purpose of the EUROSUR Regulation.

3. Identifying current gaps in access rights

Frontex has assessed the table below, which was distributed at DAPIX, providing an overview of the access rights by national authorities and Agencies and pointed to the gaps from a Frontex perspective. These comments are not meant to be exhaustive since more detailed assessment is required.

It should be noted in particular that **the founding Regulations of VIS and the agreed text on EES do not envisage at all access to the Agency's team members.**

ACCESS TO CENTRAL EU SYSTEMS FOR BORDERS AND SECURITY - CURRENT SITUATION

Schengen Information System both for EU and third country nationals primary objective: both border management and law enforcement		Other systems only for third country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				Other systems only for third country nationals primary objective: judicial cooperation
	SIS (new*)	VIS	EURODAC (new*)	EES	ETIAS (proposal)	ECRIS-TCN (proposal)
Purpose of access **Border control**[7]	*Access to categories of information*: all Possible actions: all	*Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints	*Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial image FRONTEX PROPOSES - create update, delete records on TCN having irregularly crossed the border (CAT 2)	*Access to categories of information*: all Possible actions: - Search alphanumeric data - Verify/Search fingerprints - Verify facial images - Create/Update/Delete	*Access to categories of information*: - Travel authorisation status (ok/not ok) *Possible actions*: - Search alphanumeric data	No access (where appropriate, ECRIS-TCN can inform decisions on inclusion of alerts in the SIS).
Purpose of access **Migration management: verification of identity and verification of conditions for entry or stay**	*Access to categories of information*: all but implementation is subject to national law (direct-indirect access) *Possible actions*: - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	*Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints	*Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial images FRONTEX PROPOSES: - Create, update, delete records of TCN who are staying irregularly in the Member State (CAT3)	*Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	No access	No direct access, but information may be requested through criminal records authorities where possible under national law

[7] *In the case of Eurodac the access for border control purposes refers to a situation of irregular crossing of the external border*

Schengen Information System both for EU and third country nationals primary objective: both border management and law enforcement		Other systems only for third country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				Other systems only for third country nationals primary objective: judicial cooperation
	SIS (new*)	VIS	EURODAC (new*)	EES	ETIAS (proposal)	ECRIS-TCN (proposal)
(for TCNs, in territory)	- FRONTEX PROPOSES create, update, delete alerts on TCNs for return					
Purpose of access **Return of irregular Third Country Nationals**	*Access to categories of information*: all, but implementation is subject to national law (direct-indirect access) *Possible actions*: all as defined in national law	*Access to categories of information*: all *Possible actions*: all	*Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial images - FRONTEX PROPOSES: Update the TCN record including with the date of removal or date when person has left the country.	*Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	No access	No direct access, but information may be requested through criminal records authorities where possible under national law
Specific user **Frontex EBCGT (border control tasks)**	*Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Search fingerprints - Search palm prints (legally possible, but not used) - Search facial images	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints	*Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial image FRONTEX PROPOSES: - create update, delete records on TCN having irregularly crossed the border (CAT 2)	FRONTEX PROPOSES: *Access to categories of information*: all Possible actions: - Search alphanumeric data - Verify/Search fingerprints - Verify facial images - Create/Update/Delete records	FRONTEX PROPOSES: *Access to categories of information*: - Travel authorisation status (ok/not ok) *Possible actions*: - Search alphanumeric data	No access

Schengen Information System both for EU and third country nationals primary objective: both border management and law enforcement	Other systems only for third country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement					Other systems only for third country nationals primary objective: judicial cooperation
	SIS (new*)	**VIS**	**EURODAC (new*)**	**EES**	**ETIAS (proposal)**	**ECRIS-TCN (proposal)**
Specific user **Frontex MMST (migration management tasks)**	FRONTEX PROPOSES: *Access to categories of information*: all but implementation is subject to national law (direct-indirect access) *Possible actions*: - Search alphanumeric data - Search fingerprints - Search palm prints - Search facial images - create, update, delete alerts on TCNs for return	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial images - Create, update, delete records of TCN who are staying irregularly in the Member State (CAT3)	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	No access	No access
Specific user **Frontex teams of staff involved in return-related tasks**	FRONTEX PROPOSES: *Access to categories of information*: all, but implementation is subject to national law (direct-indirect access) *Possible actions*: all as defined in national law	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: all	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search fingerprints - Search facial images - Update the TCN record including with the date of removal or date when person has left the country.	FRONTEX PROPOSES: *Access to categories of information*: all *Possible actions*: - Search alphanumeric data - Verify/Search fingerprints - Verify/Search facial images	No access	No access

Schengen Information System both for EU and third country nationals primary objective: both border management and law enforcement		Other systems only for third country nationals primary objective: border / migration / asylum management secondary (ancillary) objective: law enforcement				Other systems only for third country nationals primary objective: judicial cooperation
	SIS (new*)	VIS	EURODAC (new*)	EES	ETIAS (proposal)	ECRIS-TCN (proposal)
Specific user **EBCG Agency** For the purpose of risk analysis, vulnerability assessment and situational picture	FRONTEX PROPOSES: *Access to categories of information*: Statistical or metadata from these EU systems including those generated by their use such as searches and hits *Possible actions*: The data will be used to support risk analysis, vulnerability assessment or providing situational pictures in accordance with the Agency's mandate	FRONTEX PROPOSES: *Access to categories of information*: Statistical or metadata from these EU systems including those generated by their use such as searches and hits *Possible actions*: The data will be used to support risk analysis, vulnerability assessment or providing situational pictures in accordance with the Agency's mandate	FRONTEX PROPOSES: *Access to categories of information*: Statistical or metadata from these EU systems including those generated by their use such as searches and hits *Possible actions*: The data will be used to support risk analysis, vulnerability assessment or providing situational pictures in accordance with the Agency's mandate	FRONTEX PROPOSES: *Access to categories of information*: Statistical or metadata from these EU systems including those generated by their use such as searches and hits *Possible actions*: The data will be used to support risk analysis, vulnerability assessment or providing situational pictures in accordance with the Agency's mandate	*EBCG hosts the ETIAS central unit (see box on "issuance of travel authorisation").*	No access