Council of the European Union

Brussels, 22 May 2017
(OR. en)

9415/17

Interinstitutional File: 2016/0106 (COD)

LIMITE

FRONT 232
VISA 187
CODEC 852
COMIX 369

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council / Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland)
Subject:	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

Two political trilogues as well as nine technical meetings have been held with the European Parliament (EP) on the proposal establishing the Entry/Exit System (EES) and the proposal amending the Schengen Borders Code in connection with the EES. A third political trilogue is scheduled for 31 May 2017. It is therefore necessary to consider compromise proposals with a view to making progress on a number of issues. The proposals set out in this Presidency note build on discussions already held at the level of JHA Counsellors, both on the amendments originally proposed by the European Parliament and on those following the technical meetings. The issues tackled in this note are the following:

1. Access for the purpose of prevention, detection and investigation of terrorism or other serious criminal offences (Chapter IV);

2. Transfer of data to third countries and international organisations (Article 38) and to Member States not bound by, or not operating the EES (Article 38a);

3. Data Retention.

Delegations are invited to consider the compromise suggestions regarding these three issues, as set out below.

1. Access for the purpose of prevention, detection and investigation of terrorism or other serious criminal offences (Chapter IV)

The EP has had considerable difficulty with the amendments made by the Council to Chapter IV, on access for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences. Considering the major concerns expressed by the EP, and the importance of this Chapter to the Council, a compromise for the Chapter as a whole is proposed in the 4th column, in Annex 1 to this document.

In particular, it is proposed that the Council position would be maintained on:

(a) the reference to ‘designated authorities’ rather than ‘law enforcement authorities’;

(b) the possibility to access the EES even when the search in national databases results in a hit;

(c) the possibility to proceed to access the EES once the Prum search is launched; and

(d) the possibility to also check against refusal of entry records.

On the other hand, some amendments proposed by the EP would be broadly accepted (some with amendments), without depriving these provisions of their added value. These suggestions are in particular:

(a) limiting the urgency procedure to cases where there is an ‘imminent danger’ related to a terrorist offence or other serious criminal offence and requiring the ex post verification to take place within two working days. This should be feasible since the need to resort to this urgency procedure should be less frequent if the elements listed above are maintained for the ordinary process. It is also noted that the EP no longer insists on its initial request to require "**exceptional** cases of urgency" thus accepting the more flexible term " in a case of urgency"; and

(b) providing that there must be reasonable grounds to consider that consulting the EES will (rather than may) contribute to the detection, investigation or prevention of a terrorist/other serious criminal offence. It should be noted that 'reasonable grounds' would still be enough and certainty is not required. Moreover, a substantiated suspicion that the person falls within the scope of the EES would still be sufficient to fulfil this requirement.

The Permanent Representatives Committee is invited to provide an amended mandate to the Presidency to carry out negotiations on the basis of the compromise suggestions set out in the fourth column of the text contained in Annex 1.

2. Transfer of data to third countries and international organisations (Article 38) and to Member States not bound by, or not operating the EES (Article 38a)

The EP opposes the possibility to transfer information to third countries and international organisations for the purpose of returns, unless there is a decision by the Commission regarding the adequate protection of personal data in that third country or a binding readmission agreement. In particular, the EP opposes the possibility to transfer such information on the basis of an arrangement similar to readmission agreements, arguing that these are not binding, do not contain the necessary data protection safeguards, do not follow the institutional procedure for agreements and should therefore not be legitimised. The EP also insists on the explicit agreement and the provision of guarantees by the third country concerned to use the data only for the purposes for which it is transferred, and that such transfers should only be possible once the return decision is final, and subject to the consent of the Member State that entered the data.

The EP also maintains its position against the transfer of information to third countries or to Member States not operating, or bound by, the EES, in cases of immediate threat of terrorist or other serious criminal offences (Article 38(4a) and Article 38a), although it has shown some openness to compromise.

While reassurances have been provided that the relevant data protection legislation must still be respected (General Data Protection Regulation in case of returns/readmission and Data Protection Directive in case of terrorism/serious criminal offences), this has not proved sufficient to address the EP's concerns. The latter has also raised the concern that the conditions required for access by designated authorities of the Member States operating the EES for the purpose of their own prevention, detection and investigation of terrorist offences and other serious criminal offences (set out in Chapter IV) are not all reproduced for the transfer of such data to third countries, international organisations and Member States not operating the EES or to which the EES does not apply.

Compromise suggestions are proposed in the fourth column in Annex 2, in an attempt to address some of these concerns while maintaining the elements that are considered necessary to address operational needs.

The Permanent Representatives Committee is invited to provide an amended mandate to the Presidency to carry out negotiations on the basis of the compromise suggestions set out in the fourth column of the text contained in Annex 2.

3. Data Retention (Article 31)

The data retention period is another red line for the EP, as it is for the Council. In its position, the EP reduces the data retention period from five years to:

– four years for third-country nationals who overstay;

– two years for third country nationals who respect the period of authorised stay.

The EP has so far maintained its position and could not accept a five-year retention period for all data.

In view of the fact that this is such an important element for both co-legislators, a compromise needs to be found between the two positions. The Presidency therefore calls on delegations to provide a margin of manoeuvre on the matter for the negotiations.

Against this background, the Permanent Representatives Committee is invited to provide an amended mandate to the Presidency to carry out negotiations on the basis of which it will seek to:

– *Maintain the Council position in favour of a five-year retention period in the case of overstayers (for both the individual file and the records);*

– *Accept as a minimum, a three-year retention period in the case of non-overstayers (while every effort would, of course, be made to ensure a longer period).*

Chapter VI

Commission Proposal	~~EP position~~	Council Position	Proposed compromise text
CHAPTER IV: **Procedure and conditions for access to the EES for law enforcement purposes**	**CHAPTER IV:** **Procedure and conditions for access to the EES for law enforcement purposes**	**CHAPTER IV:** **Procedure and conditions for access to the EES for law enforcement purposes**	
Article 26 *Member States' designated law enforcement authorities*	*Article 26* *Member States' designated law enforcement authorities*	*Article 26* *Member States' designated* […] *authorities*	*Article 26* *Member States' designated authorities*
1. Member States shall designate the law enforcement authorities which are entitled to consult the data stored in the EES in order to prevent, detect and investigate terrorist offences or other serious criminal offences.	1. Member States shall designate the law enforcement authorities which are entitled to consult the data stored in the EES in order to prevent, detect and investigate terrorist offences or other serious criminal offences	1. Member States shall designate the […] authorities referred to under Article 3(1)(26a) which are entitled to consult the data stored in the EES in order to prevent, detect and investigate terrorist offences or other serious criminal offences.	1. Member States shall designate the authorities referred to under Article 3(1)(26a) which are entitled to consult the data stored in the EES in order to prevent, detect and investigate terrorist offences or other serious criminal offences.

2. Each Member State shall keep a list of the designated authorities. Each Member State shall notify in a declaration to eu-LISA and the Commission its designated authorities and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.	2. Each Member State shall keep a list of the designated authorities. Each Member State shall notify in a declaration to eu-LISA and the Commission its designated authorities and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.	2. Each Member State shall keep a list of the designated authorities. Each Member State shall notify […] eu-LISA and the Commission <u>of</u> its designated authorities and may at any time amend or replace its <u>notification.</u> […]	2. Each Member State shall keep a list of the designated authorities. Each Member State shall notify eu-LISA and the Commission of its designated authorities and may at any time amend or replace its notification. *(publication in official journal catered for in article 59)*
3. Each Member State shall designate a central access point which shall have access to the EES. The central access point shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. The central access point shall verify that the conditions to request access to the EES laid down in Article 29 are fulfilled. The designated authority and the central access point may be part of the same organisation if permitted under national law, but the central access point shall act independently when performing its tasks under this Regulation. The central access point shall be separate from the designated	3. Each Member State shall designate a central access point which shall have access to the EES. The central access point shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. The central access point shall verify that the conditions to request access to the EES laid down in Article 29 are fulfilled. The designated authority and the central access point may be part of the same organisation if permitted under national law, but the central access point shall ***be independent and*** act ~~independently~~ ***fully independently*** when performing its tasks under this Regulation. The	3. Each Member State shall designate a central access point which shall have access to the EES. […]. The central access point shall […] <u>ensure</u> that the conditions to request access to the EES laid down in Article 29 <u>of this Regulation</u> are fulfilled. The designated authority and the central access point may be part of the same organisation if permitted under national law<u>.</u> […] <u>T</u>he central access point shall act independently <u>of the designated authorities</u> when performing its tasks under this Regulation. The central access point shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification.	*Since the rest of the text refers to 'verification' it is suggested to revert to the term 'verify'.* 3. Each Member State shall designate a central access point which shall have access to the EES. The central access point shall **<u>verify</u>** that the conditions to request access to the EES laid down in Article 29 are fulfilled. The designated authority and the central access point may be part of the same organisation if permitted under national law, **<u>but</u>** the central access point shall act **<u>fully</u>** independently of the designated authorities when performing its tasks under this Regulation. The central access point shall be separate from

authorities and shall not receive instructions from them as regards the outcome of the verification. Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.	central access point shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification. Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.	Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.	the designated authorities and shall not receive instructions from them as regards the outcome of the verification **which it shall perform independently**. Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.
4. Each Member State shall notify in a declaration to eu-LISA and the Commission their central access point(s) and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.	4. Each Member State shall notify in a declaration to eu-LISA and the Commission their central access point(s) and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.	4. Each Member State shall notify […] eu-LISA and the Commission <u>of</u> its central access point and may at any time amend or replace its <u>notification</u> […].	4. Each Member State shall notify eu-LISA and the Commission of its central access point and may at any time amend or replace its notification *(publication catered for in article 59)*
5. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request access to data stored in the EES through the central access point(s).	5. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request access to data stored in the EES through the central access point(s).	5. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request access to data stored in the EES through the central access point(s).	

6. Only duly empowered staff of the central access point(s) shall be authorised to access the EES in accordance with Articles 28 and 29.	6. Only duly empowered staff of the central access point(s) shall be authorised to access the EES in accordance with Articles 28 and 29.	6. Only duly empowered staff of the central access point(s) shall be authorised to access the EES in accordance with Articles 28 and 29.	
Article 27 *Europol*	*Article 27* *Europol*	*Article 27* *Europol*	
1. Europol shall designate an authority which is authorised to request access to the EES through its designated central access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences. The designated authority shall be an operating unit of Europol.	1. Europol shall designate an authority which is authorised to request access to the EES through its designated central access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences. The designated authority shall be an operating unit of Europol.	1. Europol shall designate an authority which is authorised to request access to the EES through its designated central access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences. The designated authority shall be an operating unit of Europol.	
2. Europol shall designate a specialised unit with duly empowered Europol officials as the central access point. The central access point shall verify that the conditions to request access to the EES laid down in Article 30 are fulfilled. The central access point shall act independently when performing its tasks under this Regulation and shall not receive instructions from the designated authority referred to in paragraph 1 as regards the outcome	2. Europol shall designate a specialised unit with duly empowered Europol officials as the central access point. The central access point shall verify that the conditions to request access to the EES laid down in Article 30 are fulfilled. The central access point shall act independently when performing its tasks under this Regulation and shall not receive instructions from the designated authority referred to in paragraph 1 as regards the outcome	2. Europol shall designate a specialised unit with duly empowered Europol officials as the central access point. The central access point shall verify that the conditions to request access to the EES laid down in Article 30 are fulfilled. The central access point shall act independently when performing its tasks under this Regulation and shall not receive instructions from the designated authority referred to in paragraph 1 as regards the outcome	

of the verification.	of the verification.	of the verification.	
Article 28 *Procedure for access to the EES for law enforcement purposes*	Article 28 *Procedure for access to the EES for law enforcement purposes*	Article 28 *Procedure for access to the EES for law enforcement purposes*	
1. The operating units referred to in Article 26(5) shall submit a reasoned electronic request to the central access points referred to in Article 26(3) for access to data stored in the EES. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 29 are fulfilled. If the conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in in Article 26(5) in such a way as to not compromise the security of the data.	1. The operating units referred to in Article 26(5) shall submit a reasoned electronic request to the central access points referred to in Article 26(3) for access to data stored in the EES. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 29 are fulfilled. If the conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in in Article 26(5) in such a way as to not compromise the security of the data.	1. The operating units referred to in Article 26(5) shall submit a reasoned electronic or written request to the central access points referred to in Article 26(3) for access to data stored in the EES. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 29 are fulfilled. If the conditions for access are fulfilled, […] the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 26(5) in such a way as to not compromise the security of the data.	1. The operating units referred to in Article 26(5) shall submit a reasoned electronic or written request to the central access points referred to in Article 26(3) for access to data stored in the EES. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 29 are fulfilled. If the conditions for access are fulfilled, the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 26(5) in such a way as to not compromise the security of the data.
2. In an exceptional case of urgency, where there is a need to prevent an imminent danger associated with a terrorist offence or another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the	2. In an exceptional case of urgency, where there is a need to prevent an imminent danger associated with a terrorist offence or another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the	2. […] Where there is a need to prevent a terrorist offence or an imminent danger associated with […] another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the conditions of Article 29 are fulfilled,	**2. In a case of urgency,** where there is a need to prevent **an imminent danger associated with a terrorist offence or another** serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the conditions of

conditions of Article 29 are fulfilled, including whether an exceptional case of urgency actually existed. The ex post verification shall take place without undue delay after the processing of the request.	conditions of Article 29 are fulfilled, including whether an exceptional case of urgency actually existed. The ex post verification shall take place without undue delay ***and in any event no later than 48 hours*** after the processing of the request.	including whether a […] case of urgency actually existed. The ex post verification shall take place without undue delay after the processing of the request.	Article 29 are fulfilled, including whether a case of urgency actually existed. The ex post verification shall take place without undue delay **and in any event no later than two working days** after the processing of the request.
3. Where an ex post verification determines that the access to EES data was not justified, all the authorities that accessed such data shall erase the information accessed from the EES and shall inform the central access points of the erasure.	3. Where an ex post verification determines that the access to EES data was not justified, all the authorities that accessed such data shall erase the information accessed from the EES and shall inform the central access points of the erasure.	3. Where an ex post verification determines that the access to EES data was not justified, all the authorities that accessed such data shall erase the information accessed from the EES and shall inform the central access points of the erasure.	
Article 29 *Conditions for access to EES data by designated authorities of Member States*	Article 29 *Conditions for access to EES data by designated authorities of Member States*	Article 29 *Conditions for access to EES data by designated authorities of Member States*	
1. Designated authorities may access the EES for consultation if all of the following conditions are met:	1. Designated authorities may access the EES for consultation if all of the following conditions are met:	1. Designated authorities may access the EES for consultation if all of the following conditions are met:	

(a) access for consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence, thus making a search of the database proportionate if there is an overriding public security concer;	(a) access for consultation is necessary for the purpose of the prevention, detection~~, or~~ investigation ***or prosecution*** of a terrorist ***offence*** or another serious criminal offence~~, thus making a search of the database proportionate if there is an overriding public security concern~~	(a) access for consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence, thus making a search of the database proportionate if there is an overriding public security concern;	(a) access for consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offence or another serious criminal offence, **~~thus making a search of the database proportionate if there is an overriding public security concern~~**
(b) access for consultation is necessary in a specific case;	(b) access for consultation is necessary ***and proportionate*** in a specific case;	(b) access for consultation is necessary in a specific case;	(b) access for consultation is necessary **and proportionate** in a specific case;
(c) reasonable grounds exist to consider that the consultation of the EES data may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;	(c) ***evidence or*** reasonable grounds exist to consider that the consultation of the EES data ~~may~~ ***will*** substantially contribute to the prevention, detection***,*** ~~or~~ investigation ***or prosecution*** of any of the criminal offences in question, in particular where ~~there is a substantiated suspicion that~~ the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;	(c) reasonable grounds exist to consider that the consultation of the EES data may […] contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;	(c) evidence or reasonable grounds exist to consider that the consultation of the EES data **will** contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;

2. The access to the EES as a criminal identification tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and the following additional conditions are met:	2. The access to the EES as a ~~criminal identification~~ tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and the following additional conditions are met:	2. The access to the EES as a criminal identification tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and the following additional conditions are met:	2. The access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and the following additional conditions are met:
(a) a prior search has been conducted in national databases without success;	(a) a prior search has been conducted in national databases without success;	(a) a prior search has been conducted in national databases […]	(a) a prior search has been conducted in national databases;
(b) in the case of searches with fingerprints, a prior search has been conducted without success in the automated fingerprint verification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available.	(b) in the case of searches with fingerprints, a prior search has been conducted without success in the automated fingerprint verification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available.	(b) in the case of searches with fingerprints, a prior search has been launched […] in the automated fingerprint identification […] system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available.	(b) in the case of searches with fingerprints, a prior search has been launched in the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available.
However, that prior search does not have to be conducted where there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject. Those reasonable grounds shall be included in the	However, that prior search does not have to be conducted where there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject ***or in exceptionally urgent cases where it is necessary to***	However, the additional conditions in sub-paragraphs (a) and (b) of this paragraph shall not apply […] where there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject or	However, the additional conditions in sub-paragraphs (a) and (b) of this paragraph shall not apply where there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject or **in case of**

electronic request for comparison with EES data sent by the designated authority to the central access point(s). Since fingerprint data of visa holding third country nationals are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA provided the searches carried out in accordance with points(a) and (b) of the first subparagraph did not lead to the verification of the identity of the data subject.	***avert an imminent danger arising from a terrorist offence or other serious criminal offence***. Those reasonable grounds shall be included in the electronic request for comparison with EES data sent by the designated authority to the central access point(s). Since fingerprint data of visa holding third country nationals are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA provided the searches carried out in accordance with points(a) and (b) of the first subparagraph did not lead to the verification of the identity of the data subject.	where there is a need to prevent a terrorist offence or an imminent danger associated with another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request for comparison with EES data sent by the operational unit […] to the central access point(s). Since fingerprint data of […] third country nationals subject to a visa requirement are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA […].	**urgency** where there is a need to prevent ~~**a terrorist offence or**~~ an imminent danger associated with **a terrorist offence** or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request for comparison with EES data sent by the operating unit **of the designated authority** to the central access point(s). Since fingerprint data of third country nationals subject to a visa requirement are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA.

3. The access to the EES as a criminal intelligence tool to consult the travel history or the periods of stay in the Schengen area of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and where there is a duly justified need to consult the entry/exit records of the person concerned.	3. The access to the EES as a ~~criminal intelligence~~ tool to consult the travel history or the periods of stay in the Schengen area of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met and where there is a duly justified need to consult the entry/exit records of the person concerned.	3. The access to the EES as a criminal intelligence tool to consult the travel history or the periods of authorised stay on the territory of the Member States […] of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met. […]	3. The access to the EES as a tool to consult the travel history or the periods of authorised stay on the territory of the Member States of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met.
4. Consultation of the EES for identification shall be limited to searching in the application file with any of the following EES data:	4. Consultation of the EES for identification ***as referred to in paragraph 2*** shall be limited to searching in the application file with any of the following EES data:	4. Consultation of the EES for identification shall be limited to searching in the […] individual file with any of the following EES data:	4. Consultation of the EES for identification **as referred to in paragraph 2** shall be limited to searching in the individual file with any of the following EES data:
(a) Fingerprints (including latents) of visa exempt third country nationals;	(a) Fingerprints (including latents) of visa exempt third country nationals;	(a) Fingerprints […] of visa exempt third country nationals or of holders of a Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES;	a) Fingerprints **(including latent fingerprints)** ~~of visa exempt third country nationals or of holders of a Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES~~;
(b) Facial image.	(b) Facial image.	(b) Facial image.	

Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file as listed in Article 14(1) and Article 15(1).	Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file as listed in Article 14(1) and Article 15(1).	Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file as listed in Article 14(1), 14(6), […] Article 15(1) and Article 16(1).	Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file as listed in Article 14(1), 14(6), Article 15(1) and Article 16(1).
5. Consultation of the EES for the travel history of the third country national concerned shall be limited to searching with any of the following EES data in the individual file or in the entry/exit records:	5. Consultation of the EES for the travel history of the third country national concerned ***as referred to in paragraph 3*** shall be limited to searching with any of the following EES data in the individual file or in the entry/exit records:	5. Consultation of the EES for the travel history of the third country national concerned shall be limited to searching with any of the following EES data in the individual file,[…] in the entry/exit records or in the refusal of entry record:	5. Consultation of the EES for the travel history of the third country national concerned **as referred to in paragraph 3** shall be limited to searching with any of the following EES data in the individual file, in the entry/exit records or in the refusal of entry record:
(a) Surname(s) (family name); first name(s) (given names); date of birth, nationality or nationalities and sex;	(a) Surname(s) (family name); first name(s) (given names); date of birth, nationality or nationalities and sex;	(a) Surname(s) (family name)~~;~~, first name(s) (given names), date of birth, nationality or nationalities and/or sex;	(a) Surname(s) (family name)~~;~~, first name(s) (given names), date of birth, nationality or nationalities and/or sex;
(b) Type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;	(b) Type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;	(b) Type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;	
(c) Visa sticker number and the date of expiry of the validity of the visa.	(c) Visa sticker number and the date of expiry of the validity of the visa.	(c) Visa sticker number and the date of expiry of the validity of the visa;	

(d) Fingerprints (including latents);	(d) Fingerprints (including latents);	(d) Fingerprints. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES. […]	(d) Fingerprints, **including latent fingerprints;**
(e) Facial image;	(e) Facial image;	(e) Facial image;	
(f) Date and time of entry, entry authoriser authority and entry border crossing point;	(f) Date and time of entry, entry authoriser authority and entry border crossing point;	(f) Date and time of entry, […] authority that authorised the entry and entry border crossing point;	(f) Date and time of entry, authority that authorised the entry and entry border crossing point;
(g) Date and time of exit and exit border crossing point;	(g) Date and time of exit and exit border crossing point;	(g) Date and time of exit and exit border crossing point.	
Consultation of the EES shall, in the event of a hit, give access to the data listed in this paragraph as well as to any other data taken from the individual file and the entry/exit records including data entered in respect of revocation or extension of authorisation to stay in accordance with Article 17.	Consultation of the EES shall, in the event of a hit, give access to the data listed in this paragraph as well as to any other data taken from the individual file and the entry/exit records including data entered in respect of revocation or extension of authorisation to stay in accordance with Article 17.	Consultation of the EES shall, in the event of a hit, give access to the data listed in this paragraph as well as to any other data taken from the individual file, […] the entry/exit records and refusal of entry records including data entered in respect of revocation or extension of authorised […] stay in accordance with Article 17.	Consultation of the EES shall, in the event of a hit, give access to the data listed in this paragraph as well as to any other data taken from the individual file, the entry/exit records and refusal of entry records including data entered in respect of revocation or extension of authorised stay in accordance with Article 17.

Article 30 *Procedure and conditions for access to EES data by Europol*	*Article 30* *Procedure and conditions for access to EES data by Europol*	*Article 30* *Procedure and conditions for access to EES data by Europol*	
1. Europol shall have access to consult the EES where all the following conditions are met:	1. Europol shall have access to consult the EES where all the following conditions are met:	1. Europol shall have access to consult the EES where all the following conditions are met:	
(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate, thus making a search of the database proportionate if there is an overriding public security concern;	(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate***;*** ~~thus making a search of the database proportionate if there is an overriding public security concern;~~	(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate, thus making a search of the database proportionate if there is an overriding public security concern;	(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate
(b) the consultation is necessary in a specific case;	(b) the consultation is necessary ***and proportionate*** in a specific case;	(b) the consultation is necessary in a specific case;	(b) the consultation is necessary **and proportionate** in a specific case
(c) reasonable grounds exist to consider that the consultation may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.	(c) ***evidence or*** reasonable grounds exist to consider that the consultation ~~may~~ ***will*** substantially contribute to the prevention, detection***,*** ~~or~~ investigation ***or prosecution*** of any of the criminal offences in question, in particular where ~~there is a substantiated suspicion that~~ the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.	(c) reasonable grounds exist to consider that the consultation may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.	(c) evidence or reasonable grounds exist to consider that the consultation of the EES data **will** contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;

	1a. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed where the conditions listed in paragraph 1 are met and the consultation, as a matter of priority, of the data stored in the databases that are technically and legally accessible by Europol has not made it possible to verify the identity of the person concerned. ***Since fingerprint data of visa-holding third-country nationals are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA provided that the consultation, as a matter of priority, of the data stored in the databases that are technically and legally accessible by Europol has not made it possible to verify the identity of the person concerned.***		1a. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed where the conditions listed in paragraph 1 are met and the consultation, as a matter of priority, of the data stored in the databases that are technically and legally accessible by Europol has not made it possible to identify the person concerned. Since fingerprint data of visa-holding third-country nationals are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA.

2. The conditions laid down in Article 29 (2) to (5) shall apply accordingly.	2. The conditions laid down in Article 29 ~~(2)~~ ***(3)*** to (5) shall apply accordingly.	2. The conditions laid down in Article 29 ([…] 3) to (5) shall apply accordingly.	2. The conditions laid down in Article 29 (3) to (5) shall apply accordingly.
		2a. In addition, the access to the EES as a criminal identification tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed only if prior consultation of data stored in any information processing systems that are technically and legally accessible by Europol did not lead to the establishment of the identity of the data subject. Since fingerprint data of visa holding third country nationals are only stored in the VIS, a request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES**.** The consultation of the VIS shall be carried out in accordance with the conditions laid down in Decision 2008/633/JHA.	/ *Covered in new para 1a.*

3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the EES to the Europol central access point referred to in Article 27. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraph 1 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 27 (1) in such a way as not to compromise the security of the data.	3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the EES to the Europol central access point referred to in Article 27. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraph 1 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 27 (1) in such a way as not to compromise the security of the data.	3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the EES to the Europol central access point referred to in Article 27. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraphs 1 and 2 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 27 (1) in such a way as not to compromise the security of the data.	3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the EES to the Europol central access point referred to in Article 27. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraphs 1 and **1a** are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 27 (1) in such a way as not to compromise the security of the data.
4. The processing of information obtained by Europol from consultation with EES data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.	4. The processing of information obtained by Europol from consultation with EES data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.	4. The processing of information obtained by Europol from consultation with EES data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.	

ANNEX II

Article 38 and Article 38a

Commission Proposal	~~EP position~~	Council Position	Proposed compromise text
Article 38 *Communication of data to third countries, international organisations and private parties*	*Article 38* *Communication of data to third countries, international organisations and private parties*	*Article 38* *Communication of data to third countries, international organisations and private parties*	
1. Data stored in the EES shall not be transferred or made available to a third country, to an international organisation or any private party.	1. Data stored in the EES shall not be transferred or made available to a third country, to an international organisation or any private party.	1. Data stored in the EES shall not be transferred or made available to a third country, to an international organisation or any private party.	
2. By way of derogation from paragraph 1, the data referred to in Article 14(1)(a), (b) and (c) and Article 15(1) may be transferred or made available to a third country or to an international organisation listed in the Annex in individual cases, if necessary in order to prove the identity of third country nationals for the purpose of return, only where the following conditions are satisfied:	2. By way of derogation from paragraph 1, the data referred to in Article 14(1)(a), (b) and (c) and Article 15(1) may be transferred or made available to a third country or to an international organisation listed in the Annex in individual cases, if necessary in order to prove the identity of third country nationals for the purpose of return, only where the following conditions are satisfied:	2. By way of derogation from paragraph 1, the data referred to in Article 14(1)(a), (b)**,** […] (c) and (f) and Article 15(1)(a), (b), and (c) may be transferred or made available by border check authorities or immigration authorities to a third country or to an international organisation listed in the Annex I in individual cases, if necessary in order to prove the identity of third country nationals for the purpose of return, only where the following conditions are satisfied:	2. By way of derogation from paragraph 1, the data referred to in Article 14(1)(a), (b)**,** (c) and (f) and Article 15(1)(a), (b), and (c) may be transferred or made available **~~by~~ border check authorities or ~~immigration authorities~~** to a third country or to an international organisation listed in the Annex I in individual cases, if necessary in order to prove the identity of third country nationals for the purpose of return, only where the following conditions are satisfied:

(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 25(6) of Directive 95/46/EC, or a readmission agreement is in force between the Community and that third country, or Article 26(1)(d) of Directive 95/46/EC applies;	(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article ~~25(6)~~ ***45(3)*** of ~~Directive 95/46/EC~~ ***Regulation (EU) 2016/679***, or a readmission agreement is in force between the ~~Community~~ ***Union*** and that third country~~, or Article 26(1)(d) of Directive 95/46/EC applies~~;	(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 25(6) of Directive 95/46/EC, or a readmission agreement or any other type of similar arrangement is in force between […] the European Union or a Member State and that third country, or Article 26(1)(d) of Directive 95/46/EC applies;	(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article ~~25(6) of Directive 95/46/EC~~ ~~25(6)~~ **45(3) of Regulation (EU) 2016/679; or** (b) a readmission agreement ~~or any other type of similar arrangement~~ is in force between the European Union or a Member State and that third country; or (c) Article **49(1)(d) of Regulation (EU) 2016/679**, ~~26(1)(d) of Directive 95/46/EC~~ applies; or **(d) in situations other than those referred to in sub-paragraphs (a) to (c) provided that the following conditions are satisfied:** **i) appropriate safeguards are provided in accordance with Article 46 of Regulation (EU) 2016/679**; and **ii) the third country or international organisation agrees to use the data only for purposes for which they were provided.**

(b) the third country or international organisation agrees to use the data only for the purpose for which they were provided;	(b) the third country or international organisation ***explicitly*** agrees to use the data ***and is able to guarantee that the data are used*** only for the purpose for which they were provided;	(b) the Member State shall inform the third country or international organisation of the obligation to use the data only for purposes for which they were provided; […]	*/ (covered in para (a) above*
(c) the data are transferred or made available in accordance with the relevant provisions of Union law, in particular readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection;	(c) the data are transferred or made available in accordance with the relevant provisions of Union law, in particular ***data protection and*** readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection;	(c) the data are transferred or made available in accordance with the relevant provisions of Union law, in particular readmission agreements and transfer of personal data, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection;	~~(c)~~ **In all cases,** the data ~~are~~ **shall be** transferred or made available in accordance with the relevant provisions of Union law, in particular **data protection, including Chapter V of Regulation 2016/679 on transfers of personal data to third countries or international organisations, and** readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection;
(d) the Member State which entered the data in the EES has given its consent.	(d) the Member State which entered the data in the EES has given its consent ***and the individual concerned has been informed that his or her personal information may be shared with the authorities of a third country; and***	(d) […]	*Deletion*

	(da) a final decision ordering the return of the third-country national has been issued by the appropriate competent authority of the Member State in which the third-country national has been staying.		*Deletion*
3. Transfers of personal data to third countries or international organisations pursuant to paragraph 2 shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.	3. Transfers of personal data to third countries or international organisations pursuant to paragraph 2 shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.	3. Transfers of personal data to third countries or international organisations pursuant to paragraph 2 shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.	
4. Personal data obtained from the Central System by a Member State or by Europol for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 2(b) of Framework Decision 2008/977/JHA.	4. Personal data obtained from the Central System by a Member State or by Europol for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply if those data are further processed at national level or between Member States ~~within the meaning of Article 2(b) of Framework Decision 2008/977/JHA~~ ***pursuant to Directive (EU) 2016/680***.	4. Personal data obtained from the Central System by a Member State or by Europol for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 2(b) of Framework Decision 2008/977/JHA.	4. Personal data obtained from the Central System by a Member State or by Europol for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of ~~Article 2(b) of Framework Decision 2008/977/JHA~~ **Article 3(2) of Directive (EU) 2016/680**.

		4a. By way of derogation from paragraph 4, the data of third country nationals subject to a visa requirement referred to in Article 14(1)(a), (b) and (c) 14 (2) (a) and (b), 14 (3) (a) and (b) and the data of third country nationals exempt from visa obligation referred to under Articles 15(1) (a) 14(2) (a) and (b), 14(3) (a) and (b) may be transferred or made available by the designated authority to a third country upon a duly motivated request, only if the following cumulative conditions are met:	4a. By way of derogation from paragraph 4, the data **~~of third country nationals subject to a visa requirement~~** referred to in Article 14(1)(a), (b) and (c) 14 (2) (a) and (b), 14 (3) (a) and (b) and **~~the data of third country nationals exempt from visa obligation referred to under Articles~~** 15(1) (a) **~~14(2) (a) and (b), 14(3) (a) and (b)~~** may be transferred or made available by the designated authority to a third country **in individual cases,** ~~upon a duly motivated request,~~ only if the following cumulative conditions are met:
		(a) in an exceptional case of urgency, where there is an immediate and serious threat of a terrorist offence or other serious criminal offences as defined respectively under Article 3(1)(26) and (27) of this Regulation,	(a) **there is** an exceptional case of urgency, where there is an i~~mmediate and~~ **imminent danger associated with** ~~serious threat of~~ a terrorist offence or other serious criminal offence as defined respectively under Article 3(1)(26) and (27) of this Regulation, **(a1) the conditions referred to in Articles 28 and 29 are fulfilled.**

		(b) the transfer is carried out in accordance with the applicable conditions set under Framework Decision 2008/977/JHA.	(b) the transfer is carried out in accordance with the applicable conditions set ~~under Framework Decision 2008/977/JHA~~ out **in Directive (EU) 2016/680, in particular Chapter V thereof on transfers of personal data to third countries or international organisations**
		(c) 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.	(c) **a duly motivated written or electronic request from the third country is submitted and** 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.
		Where a transfer is based on this paragraph, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.	Where a transfer is based on this paragraph, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

		Article 38a *Conditions for communication of data to designated authorities of a Member State which does not yet operate the EES and to designated authorities of a Member State in respect of which this Regulation does not apply*	*Article 38a* *Conditions for communication of data to designated authorities of a Member State which does not yet operate the EES and to designated authorities of a Member State in respect of which this Regulation does not apply*
		1. Article 38(4) and (4a) shall apply *mutatis mutandis* to the communication of data to the designated authorities of a Member State which does not yet operate the EES and to the designated authorities of a Member State to which this Regulation does not apply, upon a duly motivated written or electronic request, provided that the reciprocal provision of any information on entry/exit records held by the requesting Member State to the Member States operating the EES is ensured.	1. Article 38(4) and (4a)**, with the exception of the reciprocity requirement in Article 38 (4a)(c),** shall apply *mutatis mutandis* to the communication of data to the designated authorities of a Member State which does not yet operate the EES and to the designated authorities of a Member State to which this Regulation does not apply, upon a duly motivated written or electronic request **and provided that Directive(EU) 2016/680 applies to that Member State. ~~provided that the reciprocal provision of any information on entry/exit records held by the requesting Member State to the Member States operating the EES is ensured.~~**

		2. In cases where information is provided pursuant to this Article, the same conditions as referred to in Article 39(1), Article 40(1) and (3), Article 43 and 52(4) shall apply *mutatis mutandis*.	2. In cases where information is provided pursuant to this Article, the same conditions as referred to in Article 39(1), Article 40(1) and (3), Article 43 and 52(4) shall apply *mutatis mutandis*