Council of the European Union

Brussels, 17 April 2023
(OR. en)

Interinstitutional File: 2022/0425(COD)

7651/2/23 REV 2

LIMITE

IXIM 57
ENFOPOL 120
AVIATION 72
DATAPROTECT 72
JAI 339
CODEC 434

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	CM 2182/23; 15719/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818 - Compilation of replies by delegations

Following the request for written contributions on the above-mentioned proposal (CM 2182/23), delegations will find in Annex a compilation of the replies as received by the General Secretariat.

This revised version contains a corrigendum received in regard to Germany's contribution.

ANNEX

WRITTEN REPLIES SUBMITTED BY DELEGATIONS

Table of Contents

BULGARIA

2022/0425 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, this Regulation lays down the rules on:

(a) the collection by air carriers of advance passenger information data ('API data') on extra EU flights and ~~selected~~ intra EU flights;

ARGUMENTS: The amendment was discussed and adopted by a majority at the last meeting.

CHAPTER 2

PROCESSING OF API DATA

Article 4

Collection, transfer and deletion of API data by air carriers

7. Air carriers shall transfer the API data both at the moment of check-in closure, that is, once the travellers can not check-in more and immediately after flight closure, that is, once the travellers have boarded the aircraft in preparation for departure and it is no longer possible for travellers to board or to leave the aircraft.

ARGUMENTS: Bulgaria's experience so far has shown that there has always been a certain point in time when the data was sent, both for PNR and API. The revision aims at facilitating monitoring procedures and balancing the costs of transfer and operational early use of PNR data. In case the data is sent at the time of check-in/check-out by the passenger, it will be significantly earlier, but will be accompanied by higher traffic and therefore data transfer costs. Data tracking, in case it is fragmented and separated by individual registration, rather than aggregated in closed registration, will be difficult in each of the chain: Air carriers-Router-PIU. When updating a passenger's registration, e.g. with luggage or a new seat, the data should be resent on the basis of Article 4.8 of the Regulation.

9. The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of API data to the router referred to in paragraph 6.

ARGUMENTS: Bulgaria's experience so far shows that such an act, which was adopted on the basis of Article 16 paragraph 3 of the PNR Directive, has been successful. We believe that a detailed regulation of the rules set out in the Regulation by means of an implementing act is more appropriate and would address more appropriately and successfully the emerging issues of implementation of the texts. So far, there have been no objections in the working group to the proposed "implementing act" and we believe that this approach more fully reflects the requirements for subsequent legislation. The reasoning is also relevant to the texts of Articles 5, 10 and 11 of this draft Regulation.

Article 5

Transmission of API data from the router to the PIUs

3. The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

CHAPTER 4

MATTERS RELATING TO THE ROUTER

Article 10

PIUs' connections to the router

1. Member States shall ensure that their PIUs are connected to the router. They shall ensure that their national systems and infrastructure for the reception and further processing of API data transferred pursuant to this Regulation are integrated with the router.

   Member States shall ensure that the connection to that router and integration with it enables their PIUs to receive and further process the API data, as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner.

2. The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 11

Air carriers' connections to the router

2. The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

CZECHIA

Chapter 1

Article 1

- In (a), the word "selected" should be deleted.
- In (c), the last phrase should read "… and intra-EU flights **selected by Member States, to be processed pursuant to Directive (EU) 2016/681**" or similarly.
- Recital 14 should clarify that Member States can "select all" intra-EU flights in cases of relevant terrorist danger as explained by the judgment C-817/19 and that the router will implement such selection immediately.

Comments:

Air carriers should be required to transmit API data on all intra-EU flights for operative reasons. It should be clear that, in accordance with judgment C-817/19, the selection of intra-EU flights is responsibility of the Member State and the processing at PIU is governed by PNR Directive.

Article 3

- Relevant definitions should be aligned with document 7753/23, including as regards correct references (e.g. definition of "crew" in point (g) should refer to point (i) of API Borders).
- In (o), the definition of "personal data" should preferably refer to **Article 3 point (1) of Directve (EU) 2016/680**, since the purpose of processing under this Regulation is to combat crime.

Chapter 2

Article 4

- Para 2 should read:

Air carriers shall collect the API data in such a manner that the API data that they **collect are transferred in their entirety and accurately** in accordance with paragraph 6 ~~is accurate, complete and up-to-date~~. **Where the air carrier becomes aware that API data it has collected have been rendered incorrect or missing before such transfer, air carrier shall without delay transfer completed or corrected API data.**

- Para 5 should read:

The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down detailed technical requirements and operational rules for the collection **and quality** of the API data referred to in Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means in accordance with paragraphs 3 and 4 of this Article.

- Para 7 should read:

Air carriers shall transfer the API data:

(a) for passengers:

(i) per passenger both at the moment of **the first** check-in**,** and

(ii) for all boarded passengers immediately after flight closure, that is, once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or to leave the aircraft**;**

(b) for all members of the crew immediately after flight closure, that is, once the crew is on board the aircraft in preparation for departure and it is no longer possible for them to leave the aircraft.

- Para 8 should read:

Without prejudice to the possibility for air carriers to retain and use the data where necessary for the normal course of their business in compliance with the applicable law, air carriers shall immediately ~~either correct, complete or update, or~~ permanently delete, the API data concerned in both of the following situations:

(a) where they become aware that the API data collected ~~is inaccurate, incomplete or no longer up-to-date or~~ was processed unlawfully, or that the data transferred does not constitute API data;

(b) where the transfer of the API data in accordance with paragraph 3 has been completed.

Where the air carriers obtain the awareness referred to in point (a) of the first subparagraph of this paragraph after having completed the transfer of the data in accordance with paragraph 6, they shall immediately inform the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). Upon receiving such information, eu-LISA shall immediately inform the PIUs that received the API data transmitted through the router.

Comments:

Para 2

As the obligations in paragraphs 2 and 4 are not data protection requirements and will not be enforced by DPAs, they should at least use different wording. The aim of this wording is to ensure that air carriers transfer API data they have as they have them. This may be particularly relevant if the aim is to stress that mere sharing of API data does not amount to border check, i.e. ensuring (or verifying) the accuracy of API data. The obligation to keep data was deleted as the timing updated needs to be aligned with timing of transfer under paragraph 7.

In compliance with the explanations of the Commission, new last sentence ensures immediate correction of unduly modified API data. This sentence could be moved to para 6 as well. Using this sentence also simplifies para 8. However, this presumes that API data are in fact "modifiable" in router through re-submission by air carrier.

New Presidency compromise proposal of Article 8a of the API Borders Regulation was considered with care, but while it may fit into the API Borders proposal, it appears quite long, requires "updates" (its paras 2 and 4) and may cause problems by requiring deletion of API data (its para 5) which would not work properly as regards PIU processing (mistake in a first name could lead to deletions). However, as some delegations were requesting longer text, CZ is ready to work with a parallel solution in the API Law Enforcement Regulation as well.

Para 5

The words "and quality" have been added to help establish reasonable level of compliance by air carriers. Necessary but reasonable level of data quality would then be tied indirectly to sanctions.

Para 7

Taken from Presidency proposal as regards API Borders Regulation, but inserted the word "first" due to the explanations of the Commission, that there should be only 2 instances of transfer – when data first become available and then after flight closure. (To prevent updates each time a seat is changed during repeated online check-ins.)

Para 8

Simplified to focus on deletion of API data.

Article 5

- Para 2 should read:

Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. Those Member States shall, in accordance with Article 2 of that Directive, regularly review and where necessary update those lists and shall immediately provide eu-LISA with any such updated lists. **Any updates shall be implemented into the router immediately.** The information contained on those lists shall be treated confidentially.

- Para 3 should read:

The Commission is empowered to adopt **implementing** acts in accordance with Article **XX** to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1 **and for sharing lists of the intra-EU flights between PIUs**.

Comments:

Para 2

New sentence should ensure that updates of the lists are swiftly implemented into the data sharing by the router.

Para 3

As this topic concerns mostly Member States and not air carriers, implementing acts are much more appropriate method of adoption of secondary legislation. In addition, sharing of lists of selected flights could be regulated in detail by such implementing act.

Chapter 3

Article 6

- Para 2 should read:

The logs referred to in paragraph 1 shall be used only for ensuring the security and integrity of the API data and the lawfulness of the processing, in particular as regards compliance with the requirements set out in this Regulation, including proceedings for penalties for infringements of those requirements in accordance with Articles 15 and 16**, and for criminal proceedings [related to terrorist offence or serious crime]**.

Comments:

Given that logs can be used not only for ensuring protection of personal data, but also for infringements of this Regulation, it would be disproportionate to exclude using these logs in criminal proceedings. If a limitation is necessary, the use of logs should cover, as a minimum, criminal proceedings for all crimes to which PNR Directive applies (see square brackets).

Article 7

- The first subparagraph should read:

The eu-LISA shall be controller, within the meaning of Article 3, point (8) of Regulation (EU) 2018/1725 in relation to the processing of API data constituting personal data under this Regulation through the router, including transmission and storage for technical reasons of that data on the router. **The PIUs shall be controllers, within the meaning of Article 3, point (8), of Directive (EU) 2016/680 in relation to their receipt and processing of API data constituting personal data under this Regulation.**

Comments:

The joint controllership of the router by dozens of PIUs, i.e. relatively small units, will be extremely unwieldy. Responsibilities of eu-LISA as a processor (under Art. 87 EUDPR) could not fully support PIUs in the entirety of their responsibilities.

National data protection authorities will have limited impact due to the inability of individual PIUs to implement any changes in reasonable time-frame. There are important responsibilities on the part of router operator and indeed, eu-LISA would in fact behave in a way similar to controllers (Art. 13 para 1). Therefore, it would be more practical to have eu-LISA as a controller supervised by EDPS.

Article 8 and Article 9

CZ proposes to delete particular references to "API data constituting personal data" in both Articles.

Comments:

First, such deletion would underline that this obligation is different from data protection obligations.

Second, the Commission is not clear whether all API data are personal data or not, and the title of the Chapter 3 does not help, because this is not clearly a data protection obligation – it is much more a data security obligation.

Third, there is really no added value in being "particular" as regards "API constituting personal data".

Fourth, air carriers and PIUs will not be required to establish two tiers of security and monitoring based on speculations as to what API data are personal data.

Chapter 4

Article 10

- Para 2 should read:

The Commission is empowered to adopt **implementing** acts in accordance with Article **XX** to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Comments:

Para 3

As this topic concerns mostly Member States rather than air carriers, implementing acts are much more appropriate method of adoption of secondary legislation.

Article 11

CZ reiterates its request that the Regulation addresses the costs of the air carriers. Recent air carrier Industry Position on the proposals for API Regulations underlined that there will be additional costs imposed on carriers related to intra-EU data collection and that it has not been demonstrated that such costs will be fully mitigated by a centralized data flows through router. Indeed, the cost of collection and transfer of API data is estimated to EUR 125 million one-off expenditure and recurrent net costs EUR 36 million yearly. Additional burden will arise in adaptation to scanning of travel documents at the gates for intra-EU flights.

Article 12

Taking into account that the Presidency is developing a new compromise proposal to Article 25 of API Borders Regulation, CZ refrains from proposing alternatives.

Article 13

Taking into account that the Presidency is developing a new compromise proposal to Article 14 of API Borders Regulation, CZ refrains from proposing alternatives.

Article 15

- Para 2 should read:

Member States shall ensure that the national supervisory authorities have all necessary means and all necessary investigative and enforcement powers to carry out their tasks under this Regulation, including by imposing the penalties referred to in Article 16 where appropriate. They shall **ensure that the exercise of the powers conferred on the national supervisory shall be subject to appropriate** ~~lay down detailed rules on the performance of those tasks and the exercise of those powers, ensuring that the performance and exercise~~ ~~is effective, proportionate and dissuasive and is subject to~~ safeguards in compliance with the fundamental rights guaranteed under Union law.

Comments:

The second sentence is too detailed and strange, as powers can be quite general and still remain effective. In particular the phrase "effective, proportionate and dissuasive" should be used in relation to sanctions, rather than in relation to official activity of supervisory authorities. It is strange and could lead to strange interpretations.

Article 16

- The first subparagraph should read:

Member States shall lay down the rules on penalties applicable to infringements of this Regulation **by air carriers** and shall take all measures necessary to ensure they are implemented. The penalties provided for shall be effective, proportionate and dissuasive penalties.

Comments:

In line with recital 23, a clarification specifies that penalties should be applicable to infringements of this Regulation by air carriers and not by eu-LISA for example.

Article 19

Since CZ proposes to change the **delegated** acts in **Articles 5(3) and 10(2)** to **implementing** acts, CZ also proposes to **delete reference to these Articles in para 2** and to introduce new Article on implementing acts.

GERMANY

Written comments following the IXIM Working Party meeting on 16/17 March 2023

General remarks:

Germany maintains its scrutiny reservation regarding the regulatory proposal.

We would like to point out that the relationship between the PNR Directive, its restrictive interpretation by the ECJ and the proposed Regulation on law enforcement appears to be in need of clarification and further regulation. This includes the following points, which we will come back to when discussing the individual provisions:

1. During data transmission from the air carriers to the Passenger Information Units (PIU) overlaps, duplications and regulatory contradictions between the PNR Directive as interpreted by the ECJ and the proposed Regulation on law enforcement are to be avoided.

2. The ECJ has limited the application of the PNR Directive in several respects for reasons of fundamental rights. We ask to check whether the restrictive requirements of the ECJ for the processing of PNR data should be included at a suitable point in the proposed regulation. We have included specific suggestions in Art. 1 and Art. 5 para. 2.

3. In the interest of legal clarity the proposed Regulation on law enforcement should provide for explicit rules regulating that the processing of API data after transmission to the PIUs is subject to the PNR Directive and the national laws implementing this Directive.

Article 1:

According to the regulatory practice chosen by the Commission, the collection of API data and its transmission first to the router and from there to the PIUs is to be regulated by the Regulation on law enforcement, while the processing is to be regulated in particular by the PNR Directive (p. 20 Impact Assessment). The question that was already addressed at the beginning arises once again, namely whether the Commission's proposal sufficiently takes into account the principles for PNR data processing developed by the ECJ in its PNR Judgement.

For example, Article 1 speaks in general terms of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, whereas the ECJ requires a connection between criminal offences and the carriage of passengers by air in the PNR context. In the interest of legal clarity it could be advisable to include this provision in Article 1 of the Regulation.

We propose the following wording:

"For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime ***having an objective direct or indirect link with the carriage of travellers by*** *air, this Regulation lays down […]."*

Why does Article 1 (a) refer to "selected intra-EU flights" while Article 2 refers to "intra-EU flights"? Are these provisions contradictory?

Article 2:

The scope of the regulation should be specified and, in the interest of legal clarity, it should be made clear that the further processing of the API data after transmission to the PIU is subject to the PNR Directive.

We propose the following wording:

"This Regulation applies to ***the collection, transfer and deletion by*** *air carriers* ***of API data*** *conducting scheduled or non-scheduled extra-EU flights or intra-EU flights* ***and to the transmission of API data to PIUs on extra-EU flights and selected intra-EU flights for subsequent processing pursuant to Directive (EU) 2016/681****."*

As is the case with Article 1 (a), this raises the question as to why the wording of the two provisions differs and why Article 1 (a) refers to "selected intra-EU flights".

Article 3:

The references to the Regulation API border management in Article 3 (g), (h), (i), (l) and (n) are incorrect. We ask for correction.

Why does the definition of "terrorist offences" differ from the regulatory practice in Article 3 (8) of the PNR Directive? Given the present context, should reference not also be made to acts sanctionable under national law within the meaning of Articles 3-12 of Directive (EU) 1017/541?

Article 4:

Paragraph 1:

In the Impact Assessment, the Commission justifies the necessity and proportionality of API data processing by stating, among other things, that the use of verified API data makes PNR data processing more reliable and effective and that false positive PNR hits can be avoided with API data. As the proposed Regulation provides for the mandatory and extensive collection of API data for the first time, we wonder whether the Commission has empirical information on the improvement of hit rates and the other assumptions which, in the Commission's view, make an expansion of data processing powers seem necessary and proportionate.

Germany asks the Commission to explain why it believes the transmission of the API data of all EU flights ("flights referred to in Article 2") to the router is in line with the ECJ's requirements, although the ECJ in its judgment of 21 June 2022 requires a limitation to certain EU flights not only for the processing of PNR data, but also for the transmission thereof, as is apparent from margin no. 174 and the operative part under no. 7 (see also the comments under margin no. 96 et seq., according to which the data transmission itself, as opposed to the storage, constitutes an independent encroachment on fundamental rights).

According to the explanations on p. 37 of the Impact Assessment, the API data are a final catalogue of data categories to be transmitted. We already pointed out for the proposed Regulation on border management that the word "only" should be added to Article 4 (1) of that Regulation for clarification. We refer to our written comments of 26 January 2023.

A provision analogous to Article 4 (1) sentence 2 is missing in the proposed Regulation on border management. The EDPS also points this out in its opinion 6/2023 of 8 February 2023. An analogous provision should be added.

In addition, to the extent that Article 4 (2) and (3) of the proposed Regulation on border management apply in the context of Article 4 (1) of the proposed Regulation on law enforcement, we refer to our written comments of 26 January 2023 following the IXIM Working Party Meeting on 11/12 January 2023.

Paragraph 2:

Where it is required that the data are "accurate, complete and up-to-date", it should not be made to seem that the air carriers are able to ensure this completely. Ultimately, the air carriers are merely able to receive the passengers' data (which is sometimes even an automated process) and do not have any sovereign powers over passengers. This should be made clearer in the provision (please refer to our written comments following the IXIM Working Party meeting on 11/12 January 2023 regarding Article 5 (1) of the proposed Regulation on border management).

We propose the following wording:

"Air carriers shall collect the API data in such a manner that the API data that they transfer in accordance with paragraph 6 is accurate, complete and up-to-date ***within the limits of the means available to them.****"*

Parapraph 3:

According to the Impact Assessment, either the passenger is to scan the machine-readable zone of their travel document in advance during online check-in, or the data is to be collected from the passenger at the airport. In the latter case, the airport staff are to automatically scan the machine-readable zone at check-in or when the passenger boards the aircraft, or the passenger is to scan in the data themselves at a self-service machine. However, these options are not mentioned in the proposed Regulation. Does the Commission intend to regulate this in delegated acts in accordance with Article 4 (4)? Considering the significant infringements of fundamental rights, should this not also be specified in the Regulation?

Insofar as paragraph 3 refers to paragraph 2 see comments on paragraph 2.

Parapraph 4:

Please explain the use of the term "secure" in the two proposed Regulations and, in particular, the relationship between Article 8 of the proposed Regulation on law enforcement and Article 17 of the proposed Regulation on border management. Why does the content of these two provisions differ for their different addressees? Is it not necessary for both proposed Regulations to provide for rules for all of their addressees?

In this respect, we refer to our comments below on Art. 10.

Paragraph 6:

We still have many questions regarding the proposal to introduce a central router and we still see many problems, which need to be examined more closely. We therefore maintain a broad scrutiny reservation regarding the entire router solution. We pointed out important aspects of this in our written comments of 26 January 2023 and 6 February 2023. We have not yet received an adequate response to these questions.

The coexistence of the proposed Regulation on law enforcement and the PNR Directive results in the API data being routed to the PIUs via the central router under this proposed Regulation, whereas the PNR data (which also include the API data) are still to be transmitted by the air carriers directly to the PIUs under the PNR Directive. This coexistence of two different systems that overlap in their scope still seems questionable.

In the IXIM Working Party meeting on 11/12 January 2023, the Commission explained that, under current law, there is already the possibility for the central router to also be used by Member States to transmit PNR data under the PNR Directive in line with Article 16 (4) of Regulation (EU) 2018/1726. We kindly ask once again for an explanation of the following: How would the use of the router to transmit PNR data be compatible with the PNR Directive, which states that the national PIU (and not eu-LISA) is responsible for collecting PNR data from air carriers (Article 4 (1) of the PNR Directive) and that Member States must ensure that air carriers transmit PNR data to the database of the PIU (Article 8 (1) sentence 1 of the PNR Directive)? The detailed requirements regarding the router in Chapters 3 and 5 of the proposed Regulation on border management and in Chapter 4 on data protection do not apply to the transmission of PNR data. What would be the legal relationship between the air carriers, eu-LISA and the PNR PIUs? Would this relationship be shaped solely by the agreement referred to in Article 16 (4) of Regulation (EU) 2018/1726 or would, in the view of the Commission, other EU or national provisions also apply? In the Commission's view, would it be sufficient for the relationship to be shaped exclusively by a single relevant agreement?

From an operational perspective, the question remains as to whether it is guaranteed that the data transmitted by the air carriers can be processed in the Member States without any issues. This would absolutely require unified use of existing standards. It would have to be ensured that air carriers transmit API data to the router in a manner that is compliant with the standard and using established message formats so that API data are always transmitted to the router with uniform content and structure, regardless of which air carrier transmits the data. In addition, the question of whether the international standards can be improved should be examined. We refer to Germany's comments of 23 February 2023 regarding this. In Germany's view, it would be necessary to execute these specifications as part of an implementing act. According to the interinstitutional agreement "Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union" of 18 June 2019, measures establishing a procedure to ensure the uniform implementation of a rule laid down in the basic act are to be adopted by means of implementing acts. There is no situation here in which the Commission should be given the power to change or add to the legal act. In this respect, Germany believes that the specification of concrete requirements for API data transmission should take place in the form of an implementing act. Another reason for this is that there must be relevant possibilities for Member States to exert influence on this key issue.

In order to ensure compliance with the standard, the router would need to have a technical component that automatically detects any deviations from the binding standard (measurement of compliance with standard) and automatically provides the air carriers with corresponding feedback without actually providing eu-LISA with access to the data.

We propose the following wording:

"Air carriers shall transfer the API data collected pursuant to paragraph 1 to the router, by electronic means. They shall do so in accordance with the detailed rules referred to in paragraph 9, where such rules have been adopted and are applicable. ***The router measures the compliance with the detailed rules referred to in paragraph 9 by means of an automated procedure without allowing access to the data and provides automated feedback to air carriers in case of any deviations."***

Germany recalls the Commission's announcement that it would investigate what the practical and legal consequences of providing real-time flight information via the central routing mechanism would be. In this context, we also asked the Commission for an assessment of whether, in the Commission's view, the provision of such information would be in line with the principle of subsidiarity, whether it would be necessary and proportionate, and whether it was also otherwise considered legally and practically feasible. Is the Commission able to provide an assessment on this?

Paragraph 6 sentence 1 is limited to the statement that the data must be transmitted electronically from the air carriers to the router. Here it is unclear to whom the legal obligation to transmit the data applies. We already pointed this out with regard to Article 6 of the proposed Regulation on border management. If we correctly understood the Commission's explanations in the context of the IXIM Working Party meeting on 11/12 January 2023, the obligation to transmit data is to apply to the Member States or the authorities of the Member States, and not to the EU (eu-LISA). In Germany's view, a clarification in the Regulation is also important with regard to Article 16, which obliges Member States to impose sanctions on air carriers which violate the Regulation.

Parapraph 7:

Depending on the air carrier, check-in is available as early as 72 hours prior to departure. We would like to point out that compliance with an obligation to transmit API data at a point in time that varies for each passenger cannot be verified by the national supervisory authority pursuant to Article 15.

Parapraph 8:

The wording in paragraph 8 (a) differs from the comparable provision in Article 6 (4) of the proposed Regulation on border management. This should be remedied by deleting the word "transferred".

Regarding paragraph 8 (b): We understand the provision to the effect that it provides for an obligation to delete the data after the transmission has been completed. This should be regulated clearly in the wording.

The reference to paragraph 3 seems misleading, as the data transmission is regulated in paragraph 6.

We propose the following wording of paragraph 8 (b):

"Without prejudice to the possibility for air carriers to retain and use the data where necessary for the normal course of their business in compliance with the applicable law, air carriers shall

*(a) immediately either correct, complete or update, or permanently delete, the API data concerned ~~where~~ **when** they become aware that the API data collected is inaccurate, incomplete or no longer up-to-date or was processed unlawfully, or that the data ~~transferred~~ does not constitute API data;*

*(b) ~~where~~ **immediately and permanently delete the API data when** the transfer of the API that data in accordance with paragraph ~~3~~**6** has been completed."*

Furthermore, we reiterate our questions regarding Article 8 (1) of the proposed Regulation on border management. We kindly ask the Commission to explain the necessity of storing the API data with the air carriers after transmission to the router within the framework of the proposed Regulation on border management. How does the rule relate to the present provision, according to which the data are to be deleted after they have been completely transmitted to the router? Surely (apart from certain exceptional cases of divergent scopes of the two proposed Regulations) these are the same data sets?

Parapraph 9:

Our comments on paragraph 6 apply here, too. We propose the following wording:

"The Commission shall adopt an implementing act to *~~The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by~~ lay~~ing~~ down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of API data to the router referred to in paragraph 6.* ***The aim of these detailed rules is to ensure a standardised data delivery by the air carriers. In particular, deviations from the standard are to be excluded and the mandatory use of specific IATA/ICAO-Codes is to be prescribed, so that all air carriers transmit API data in a uniform manner."***

Article 5

Paragraph 1:

For clarification, paragraph 1 should state that the router forwards the API data to the PIU without any changes.

We propose the following wording:

"The router shall, immediately and in an automated manner, transmit the API data, transferred to it by air carriers pursuant to Article 4, to the PIUs of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, or to both in the case of intra-EU-flights. ***The router shall not modify the API data transmitted by air carriers.*** *Where a flight has one or more stop-overs at the territory of other Member States than the one from which it departed, the router shall transmit the API data to the PIUs of all the Member States concerned."*

Would it not be better for the reference to Article 4 to also name the specific relevant paragraphs (paragraphs 6 and 7)?

Would the term "states" be better than "countries"?

Parapraph 2:

In its PNR Judgement, the ECJ, interpreting the PNR Directive in a manner consistent with fundamental rights, sets out specific requirements for selecting EU flights for which PNR data on intra-EU routes may be processed (cf. para. 174 of the judgment and para. 7 of the operative provisions of the judgment). We ask to check whether these requirements, which have not yet been reflected in the text of the PNR Directive or in the text of the present draft, should be included in the text for the sake of legal clarity.

Should a flight route be identified at short notice as a risk route thus as a "selected intra-EU flight", it must be ensured that the corresponding API data transmissions relevant for the control of the flight route are technically implemented very quickly, ideally immediately. For this reason, paragraph 2 should contain an explanation that the standard-compliant data transmission for intra-EU routes must start immediately after eu-LISA has been notified.

We propose the following wording of paragraph 2:

"Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. **The decision to extend the application of that Directive to intra-EU flights presupposes a threat assessment by the respective Member State finding that there is a threat linked to terrorist offences and serious crime which is capable of justifying the application of that directive to intra-EU flights and that the extension is absolutely necessary for the purposes of attaining the objective set out in Article 1(2) of Directive (EU) 2016/681. In the absence of a genuine and foreseeable terrorist threat with which the Member State concerned is confronted, the application of the system established by Directive 2016/681 must be limited to the transfer and processing of the PNR data of selected flights relating, inter alia, to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application.**

Those Member States shall, in accordance with Article 2 of ~~that~~ Directive **(EU) 2016/681**, regularly review and where necessary update those **lists in accordance with changes in the circumstances that justified their selection** and shall immediately provide eu-LISA with any such updated lists. The information contained on those lists shall be treated confidentially.

After receiving the list by a Member State, eu-LISA shall ensure that the data transmission in line with the applicable standard and in accordance with paragraph 1 for the flights contained in the list is started immediately."

Article 6:

Why does Article 6 not have any requirements for storing log data with regard to the PIUs, even though the wording of Article 9 ("their ... obligations ... as regards their processing of API data constituting personal data, including ...") is based on the premise that the PIUs too process personal data and obligates them to self-monitoring and verification of the log data ("including through frequent verification of the logs in accordance with Article 7")? We ask the Commission to explain.

Paragraph 1:

Why are the requirements for eu-LISA with regard to the keeping of logs in Article 13 (1) of the proposed Regulation on API for border management more specific than those for air carriers in Article 13 (2) of the same proposed Regulation and in Article 6 (1) of the proposed Regulation on API for law enforcement? Shouldn't the requirements have the same degree of detail, especially since the log data are also intended to serve as evidence that the air carriers have (or have not) met their obligations under the API regulation (compare Article 1 (2) of the proposed API law enforcement regulation)?

For air carriers, we ask in any case that an exclusion for personal data be included which is comparable to the one in Article 13 (1) (e) of the API border management regulation.

Paragraph 4:

Insofar as paragraph 4 subparagraph 2 is intended to allow air carriers under certain conditions to keep the logs longer ("may"), Germany believes it would be preferable to replace the word "may" with the word "shall".

Article 7:

Despite the position of the EDPS, we doubt whether it is compatible with Article 4 (7) of the GDPR for PIUs and the air carriers to be solely responsible under data protection law for data processing (Article 7) and for eu-LISA to be only the processor (Article 16 API border management), because the router is IT infrastructure operated by eu-LISA, which is solely responsible for its specific design, over which the PIUs and air carriers have no influence.

Furthermore, processing on behalf of a controller means that the controller must be able to influence the processor. That is not the case in the constellation envisaged here. In addition, the fact that eu-LISA is not responsible for the content or lawfulness of the data indicates that this is not a case of processing on behalf of a controller. The rulings of the European Court of Justice recognise that an entity may be a (co-)processor even if it has no access to the data itself.

Article 8:

We ask for an explanation why this Article assigns legal obligations to eu-LISA, which is only the processor, and why these obligations otherwise apply to the controllers? In our view, this contradicts eu-LISA's intended role as processor.

With regard to Article 17 of the proposed API border management regulation, the Commission stated that this phrase was found in other legislative acts too, and that the only difference was that eu-LISA was the controller there. This explanation shows that eu-LISA's apparent role here as processor is only a fiction that does not reflect the actual situation, and that – as in the other legislative acts – eu-LISA is actually the controller here too.

Please explain the relationship of Article 8 of the proposed API law enforcement regulation to Article 17 of the proposed API border management regulation. Why does the content of these two provisions differ for their various addressees? Is it not necessary for both proposed regulations to provide for rules for all of their addressees?

Based on the recommendation of the EDPS regarding the security of API data (see Opinion 6/2023 of 8 February 2023, nos. 26 to 27, and Recommendation no. 3), we propose including a reference in Article 8 to the relevant provisions on security in the proposal for an API border management regulation (Article 17 (1) sentence 1 and Article 17 (2)) in order to clarify that eu-LISA's obligations to ensure the secure processing of API data for law enforcement purposes comply with Article 17 of the proposed API border management regulation. We also propose including a statement on general data protection law and clarifying that Article 8 does not affect the provisions of Directive (EU) 2018/680.

Article 9:

We wonder whether the data protection provision in Article 9 is consistent and sufficient. We refer first of all to our request for explanation of Article 6 with regard to the PIUs and ask the Commission further to explain why Article 9 refers to Article 7 rather than Article 6, and how this reference should be understood.

We also ask for an explanation of which specific data protection obligations are supposed to apply, in addition to those in Article 8 of this proposal, to the processing of API data, in particular according to the Union legislative acts mentioned in recitals 5 and 17. We believe that the complex interrelationship of the relevant Union legislative acts should not only be mentioned in the recitals, but should also be addressed in the regulation itself.

We also ask the Commission why the proposed API law enforcement regulation has no provision on personal data protection audits for the PIUs, corresponding to Article 19 (1) of the proposed API border management regulation.

Article 10:

We have a question about how to understand this Article. We assume that the Member States are responsible for deciding on the specific technical details for their national connection to the router. Would it be possible for the Member States to provide only for one technical connection to the router and to have a technical services provider who acts as processor for both areas, i.e. border management and law enforcement, and forwards the data according to their purpose to the competent border authority or PIU for further processing? We believe it would be helpful to make this clear in the text of the regulation.

Article 10 (1) subparagraph 2 uses the wording "to receive and further process the API data, as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner". Regarding the corresponding provision in the API border management regulation (Article 20), the Commission explained at the IXIM Working Party meeting on 23 January 2021 that the term "secure" should be understood in the meaning of Article 17 of the API border management regulation. In response, Germany proposed the following clarification of Article 20 of the API border management regulation (proposed wording: "in a manner that is lawful, effective and swift while ensuring security within the meaning of Article 17"; see our written comments for the IXIM Working Party dated 8 February 2023).

By contrast, at the IXIM Working Party meeting on 16/17 March 2023, in discussing Article 4 (4) of the API law enforcement regulation, which states that "Any automated means used by air carriers to collect API data under this Regulation shall be reliable, secure and up-to-date", the Commission explained that the term "secure" meant that the data must be encrypted.

Because the terms “secure” and “security” are used multiple times in the API law enforcement regulation (Article 4 (4), Article 11 (1) subparagraph 1, and Article 8) and in the API border management regulation (Article 5 (3), Article 20 subparagraph 2, Article 21 (1) subparagraph 2, Article 23 (2) and Article 28 (1), as well as Article 11: Security), we ask whether the same term is in fact intended to mean different things.

Article 11:

We refer to our comments on Article 10.

Article 13:

Paragraph 2:

If, according to paragraph 2, the Member States are to notify the air carriers in the event of technical failures, this could conflict with the need for confidentiality for selected intra-EU routes. Contacting air carriers could in some cases partly reveal the selected routes. We ask the Commission to explain whether this aspect was noted and any alternatives considered.

Paragraph 3:

If the obligation to collect and transmit API data is suspended due to a technical impossibility, this would also apply in situations when the technical impossibility can be resolved before the aircraft’s scheduled arrival in a Member State and before its scheduled departure from that Member State. In these cases, the API data could be useful for law enforcement purposes, and the further processing of the data of all passengers affected would be permitted during the time period referred to, also according to Article 6 (2) (a) of the PNR Directive; after that time period, however, collecting, transmitting and storing the data would not be proportionate. We therefore propose modifying the text accordingly to enable the transmission of data up to the time of scheduled arrival in a Member State or before the scheduled departure from that Member State, in accordance with Article 6 of the PNR Directive and in agreement with the requirements of the European Court of Justice in its judgment on PNR.

Article 14:

We raised various questions concerning the liability provision in Article 26 of the API border management regulation and thank the Commission for offering to examine these questions. Examining the provision again in the context of the present proposal has raised further questions about Member States' liability. Our questions are as follows:

1. Why should the Member States and the air carriers be liable for damage? Does the existing non-contractual liability law of the Member States not suffice? What need for regulation is behind the provision? Which use cases are meant.

2. Which law applies to assessing the damage? Is the assessment of damage based directly on Union law (which one?) or on Member State indemnity law which is applicable by way of subsidiarity? Similar liability provisions usually specify which law applies (see for example Article 20 of Regulation (EU) 2019/816, Article 46 of Regulation (EU) 2019/817, Article 46 of Regulation (EU) 2019/818, Article 58 of Regulation (EU) 2018/1861). Why does the proposal not contain such a provision?

3. Why was (non-contractual) liability not based on fault or negligence chosen? German law of compensation follows the principle of liability based on fault.

4. Who is entitled to claim damage – every potential injured party or only eu-LISA (as far as it has legal capacity)?

5. Why is a liability provision vis-à-vis the Member States needed? What regulatory need is this provision based on? Which concrete scenarios is the provision intended for?

Article 15:

We understood the Commission's explanations at the IXIM Working Party meeting on 16/17 March 2023 to mean that the wording of Article 15 was supposed to take into account the Member States' differing needs. We nonetheless ask for clarification whether the national supervisory authority and the PIU can be one and the same or at least do not have to be separate agencies.

We propose adding the following sentence 2 to paragraph 1: „***The national supervisory authority may be identical with the PIU***."

The previous request for an addition to paragraph 1 requires a change to paragraph 4. The proposed clarification in paragraph 1 should not refer to the data protection supervision; in particular, it should not undermine the existing related organisational obligations of the GDPR and the JHA Directive. In conjunction with our proposed addition to paragraph 1, we therefore propose revising paragraph 4 as follows: „*This Article is without prejudice to* ***the provisions concerning*** *powers of the supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679* […]".

Article 16:

The wording of Article 16 (1) sentence 2 differs slightly from that of Article 30 (1) sentence 1 of the proposed API border management regulation ("The penalties provided for shall be effective, proportionate and dissuasive"). We assume that this is an editorial error and ask for it to be corrected.

Article 17:

As in the case of Article 32 of the proposed API border management regulation, we ask whether only parts of the handbooks should be published.

Chapter 6

We propose inserting the following article before Article 18 in Chapter 6:

[Article XX]

Relationship to other instruments

The provisions of this regulation shall prevail over provisions of Directive (EU) 2016/681. For the subsequent processing of data and other matters not specifically covered by this Regulation the rules of that Directive shall apply.

In Germany's view, a provision explicitly governing the relationship of the API law enforcement regulation to the PNR Directive could clear up a number of ambiguities.

Article 19:

In the Interinstitutional Agreement on Better Law-Making, the standard clauses on adopting delegated acts provide for setting a time period for objections from the European Parliament and the Council following the adoption of the act. This time period is usually two months.

„A delegated act adopted pursuant to Article(s) … shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council." (Standard clause according to Interinstitutional Agreement of 13 April 2016 on Better Law-Making, Appendix, Article A, Option 3, paragraph 6).

Article 20:

We believe it is necessary to specify which data are to be transmitted to the Commission according to Article 20 (2). What kind of information does this mean exactly?

Why does paragraph 2 not state that no personal data are to be transmitted?

With regard to Article 20 (2) sentence 2, we refer to our written comments on Article 38 (6) of the API border management regulation dated 17 March 2023.

ESTONIA

EE proposals regarding to COM (2022) 731 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU)

2019/818

Please find below in **bold underlined** the text proposed by EE and in ~~strikethrough~~ the deletions of current wording.

Our proposals on the respective Articles are following:

Article 1

Subject matter

For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, this Regulation lays down the rules on:

(a) the collection by air carriers of advance passenger information data ('API data') on extra EU flights and selected intra EU flights;

(b) the transfer by air carriers to the router of the API data;

(c) the transmission from the router to the Passenger Information Units ('PIUs') of the API data on extra-EU flights and selected intra-EU flights.

Justification: Air carriers must collect passenger information data on all intra EU flights, since the lists on selected intra-EU flights are not provided to air carriers. When such lists are not shared with the air carriers, they should therefore be required to collect API data on all flights covered by this Regulation, including all intra EU flights, and then transfer it to the router, where the necessary selection should be enacted.

Article 5

Transmission of API data from the router to the PIUs

1. The router shall, immediately and in an automated manner, transmit the API data, transferred to it by air carriers pursuant to Article 4, to the PIUs of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, or to both in the case of intra-EU-flights. Where a flight has one or more stop-overs at the territory of other Member States than the one from which it departed, the router shall transmit the API data to the PIUs of all the Member States concerned.

   For the purpose of such transmission, eu-LISA shall establish and keep up-to-date a table of correspondence between the different airports of origin and destination and the countries to which they belong**.**

   However, for intra-EU flights, the router shall only transmit the API data to that PIU in respect of the flights included in the list referred to in paragraph 2.

   The router shall transmit the API data in accordance with the detailed rules referred to in paragraph 3, where such rules have been adopted and are applicable.

2. Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. Those Member States shall, in accordance with Article 2 of that Directive, regularly review and where necessary update those lists and shall immediately provide eu-LISA with any such updated lists. The **documents which** ~~information~~ contain~~ed on~~ those lists shall be treated ~~confidentially~~ **as classified documents and bear classification marking RESTREINT UE/EU RESTRICTED.**

3. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

Justification: Since the documents containing the lists of the selected intra EU flights should be confidential, these documents must be treated as such. Otherwise, the confidentiality of the document would not be guaranteed. The classification marking is necessary to achieve the purpose of the Regulation, aiming that the corresponding lists do not fall into the hands of third parties.

Article 12

Member States' costs

~~1. Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union.~~

~~However, the following costs shall be excluded and be borne by the Member States:~~

~~(a) costs for project management, including costs for meetings, missions and offices;~~

~~(b) costs for the hosting of national information technology (IT) systems, including costs for space, implementation, electricity and cooling;~~

~~(c) costs for the operation of national IT systems, including operators and support contracts;~~

~~(d) costs for the design, development, implementation, operation and maintenance of national communication networks.~~

~~2. Member States shall also bear the costs arising from the administration, use and maintenance of their connections to and integration with the router.~~

1. Costs incurred by Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union. The funding shall be released from the thematic facility of Internal Security Fund, in particular in a form of specific action. Rules and procedures used for Internal Security Fund shall be used.

OR

1. Costs incurred by Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union. The funding shall be released from the relevant Funds or Instruments under applicable rules.

Justification: The EC has previously promised to avoid the restrictions that were stipulated in the regulations of the EES and the ETIAS. Yet similar provisions which have proven to be problematic in financing of the systems have been foreseen for API regulations. We consider it necessary to avoid wording in the regulation, which may create disputes on the eligibility of the use of EU funds during the implementation of projects, limit the options developed to simplify the use of the funds and cause additional administrative burden for Member States. As the conditions for the implementation of EU funds have already been agreed (ISF Regulation 2021/1149 (EU) and BMVI Regulation 2021/1148 (EU) and Common Provision Regulation 2021/1060 (EU)), we find that setting additional restrictions in other legislation does not provide any added value in terms of protecting the EU's financial interests or ensuring internal security.

The costs incurred by the Member State in connection with establishing and integrating the connection with the router are planned to be covered by the BMVI and the ISF as well as by the 2028+ period successor HOME funds. We consider it necessary that, in order to fulfill the obligations of the Member States stated in Article 10, the possibility to apply for funds from the BMVI and ISF Thematic Facility shall be foreseen in current funding period, since the obligation in question was not known at the time of the programming of the funds. The EC applies for the same justification in the financial statement of the proposal where it is stated that BMVI Thematic Facility will be decreased in order to reinforce eu-LISA's and DG HOME's budget. It is only fair that the same approach will be taken for Member States. It is also important to emphasize that both the BMVI and the ISF allocation to Estonia have already been fully planned according to the programming rules, therefore we find it necessary to allocate additional funds to the member states for the implementation of all new initiatives.

EE would like to draw attention to the issue that the EC has not proposed to amend fund regulations as was done by the ETIAS regulation. Therefore, it is unclear how and on what legal basis the Thematic Facilities will be decreased.

Last but not least, EE considers its proposal already a compromise. In the period of 2014-2020, the ETIAS top-up was 100% of EU support. According to the BMVI and ISF regulations the maximum EU support for the Specific Action can be 90%. 100% support is only possible for emergency assistance, for actions in accordance with Article 85(2) or (3) of Regulation (EU) 2018/1240 and for operating support. In case other Member States would like to seek for 100% of EU support, the BMVI and ISF regulations must be amended, in which case EE is open for discussions.

IRELAND

Chapter 1

GENERAL PROVISIONS

Article 1

Subject matter

As a point of information, in accordance with Article 3 of Protocol (No 21) on the position of Ireland in respect of the area of freedom, security and justice, (annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union), the Irish Department of Justice is currently working to secure the required national parliamentary consent to "opt in" to this regulation, and then intends to notify the Commission of its wish to take part in the adoption and application of this Regulation.

CHAPTER 3

LOGGING, PERSONAL DATA PROTECTION AND SECURITY

Article 7

Personal data controllers

Ireland shares MS concerns regarding the designation of euLISA as Data Processor and not as Data Controller/joint Data Controller. IE requests that CION provide further explanatory information regarding the decision to designate euLISA as Data Processor for the processing of API data constituting personal data through the router in accordance with this Regulation and Regulation 729 (22).

Article 9

Self-monitoring

Ireland requests clarification and further details regarding the obligation set in Art. 9 that "the PIUs shall monitor their compliance with their respective obligations under this Regulation, in particular as regards their processing of API data constituting personal data."

CHAPTER 4

MATTERS RELATING TO THE ROUTER

Article 12

Member States' costs

Art. 12(1) states "Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union." CION indicated at the most recent IXIM that the Internal Security Fund (ISF) is the specific thematic funding instrument that will be utilised for this measure.

Ireland requests that the use of the ISF is confirmed by CION.

CHAPTER 5

SUPERVISION, PENALTIES AND HANDBOOK

Article 15

National supervisory authority

Ireland is considering the implications of this Article at national level.

Article 16

Penalties

Ireland recognises the value of introducing a penalty schedule applicable to infringements of the Regulation and remains open to hearing further details of proposals to establish a harmonised penalty schedule.

CHAPTER 6

RELATIONSHIP TO OTHER EXISTING INSTRUMENTS

Article 18(2) states:

"2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. eu-LISA shall also collect the data and statistics from the router referred to in Article 13(1) of Regulation (EU) …/… * [this Regulation]. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 74 of Regulation (EU) 2018/1862, Article 32 of Regulation (EU) 2019/816 and Article 13(1) of Regulation (EU) …/… * [this Regulation]."

Article 13(1) states:

Article 13

"Actions in case of technical impossibility to use the router

1. Where it is technically impossible to use the router to transmit API data because of a failure of the router, eu-LISA shall immediately notify the air carriers and PIUs of that technical impossibility in an automated manner. In that case, eu-LISA shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period."

As Article 13(1) is concerned with actions in case of technical impossibility to use the router, and contains no reference to statistics or reporting, Ireland queries whether Article 18(2) is incorrectly worded in its current form.

GREECE

CHAPTER 1: GENERAL PROVISIONS

Article 1 points (a) and (b): In light of Recital 16 of this Proposal *"...they (air carriers) should therefore be required to collect API data on all flights covered by this Regulation, including all intra-EU flights, and then transfer it to the router, where the necessary selection should be enacted.*", for clarity reasons, we propose the following wording changes:

(a) the collection by air carriers of advance passenger information data ('API data') **on all extra-EU and intra-EU flights** [instead of "*on extra EU flights and selected intra EU flights*"];

(b) the transfer by air carriers to the router of **all collected** API data; [instead of "*the*"].

For the same reasons, the precondition of Recital 7 that states "*insofar as those flights have been selected in accordance with Directive (EU) 2016/681*" should be deleted, since it refers to the collection of data by the air carriers, hence being not applicable.

Article 1 point (c): Adhering to our previous contributions, regarding intra-EU flights, Hellenic PiU does not see the reason why the Proposal designates eu-LISA as the one responsible for transmitting data only for selected intra-EU flights and deleting the remaining data immediately. That procedure could take place on a MS-level for the following reasons:

- The Commission supports the position that deletion will be done by the router in an automated way, without any human intervention and that such actions performed by the PIUs would be considered as processing, hence not in alignment with the provisions of the CJEU judgement.

- Though, according to Article 6 (1) and Article 13 (4) of the PNR Directive, which remain valid after the CJEU judgment, **the PIUs are already the ones that delete immediately and permanently upon receipt PNR data** transferred by air carriers that include data other than those listed in Annex I of that Directive, as well as **PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.** In this way, it is considered that Member States "*prohibit the processing*" of such data (Article 13 par. 4 of PNR Directive).

- It is noted that the deletion procedure mentioned above already takes place by the PIUs without any human intervention, operated in an automated way by MSs PNR system, hence not allowing any processing to the PIU operators or even to the IT team supporting the PIU for any reason whatsoever.

- The Commission is kindly invited to provide further clarifications, indicating the exact points of the invoked CJEU judgment that provide for the actions at stake not to be operated by the PIUs.

- Operational obligations emerge for **the PIUs that are unnecessarily required to report to eu-LISA the list of selected intra-EU flights**, keeping that list constantly updated.

- Moreover, **PIUs are also obliged to monitor eu-LISA's updated transmissions upon any changes made in the lists of selected flights** by the PIUs, so that any transmitted data for recently selected intra-EU flights are not accidentally deleted. In such a case, if the provisions of the Proposal remain as they currently are, it is not determined where does the liability stand and who need to take actions for requesting the carrier to re-transmit the erroneously deleted data.

- In the discussions that took place after the CJEU judgement, it was determined that the **filtering of data for intra-EU flights** will take place in a MS level. According to the provisions of the PNR Directive, this process **already takes place in a MS level for PNR data**. Once again, this procedure is done without any human intervention, in an automated way by MSs PNR system, hence not allowing any processing to the PIU operators or even to the IT team supporting the PIU for any reason whatsoever. Yet, this Proposal suggests this process to take place in eu-LISA, instead of the PIUs. Thus, there is a conflict in these two procedures, which does not seem to be in alignment, inter alia, with the principle of subsidiarity.

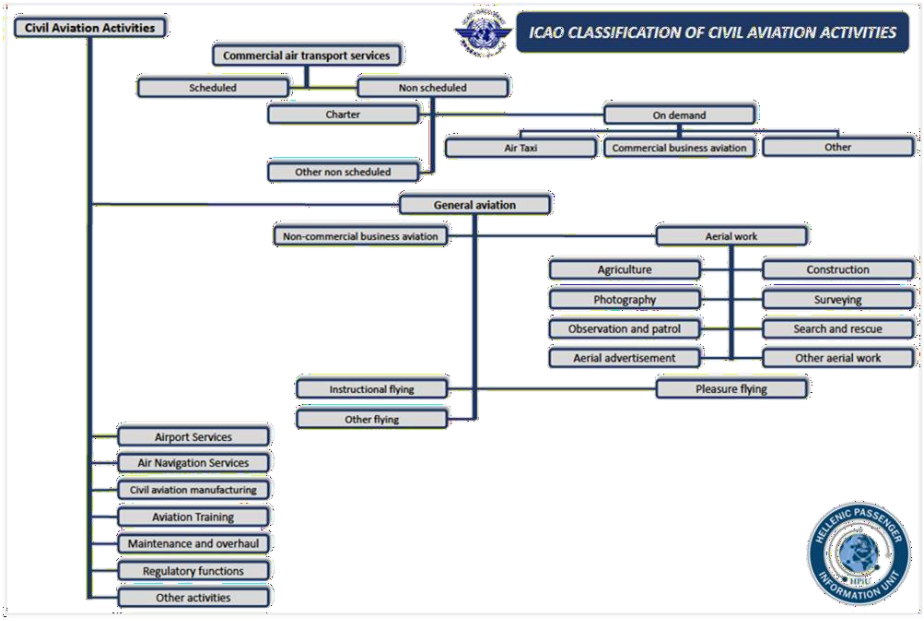
  Besides, API data is only a part of the PNR data, according to the PNR Directive. It could be rather controversial for the PIUs to align with the provisions, which refer to a subtotal of their main data set (PNR data).

- **Eu-LISA should have the role of a technological "partner"** and engage in monitoring the lawfulness of data processing only as regards its personnel. By being provided with the responsibility of data erasure for non-selected intra-EU flights, eu- LISA also **takes up the role of an authority supervising PIUs in terms of not processing data** for such flights, as if there are not legally specified independent authorities to perform such audits on MS-level.

Taking the above into consideration, we propose the following wording chance: (c) the transmission from the router to the relevant Passenger Information Units ('PIUs') of **all received** API data. [instead of "*the API data on extra-EU flights and selected intra-EU flights*"].

Acceptance of our position would also entail changes in Article 5 (noted further below) and Recital 14 of this Regulation, as well as Article 12 of Regulation [API Border].

Article 3 points (d) and (e): While the definition of scheduled flights seems to be precise, the definition of non-scheduled flights needs to be further clarified. Specifically, despite the fact that the Impact Assessment Report accompanying the two API Proposals contain multiple references of the term "*commercial air carrier*", in the definition of non-scheduled flights, it is not clear if the scope includes only commercial air transport services (in the meaning of ICAO Classification of Civil Aviation Activities) i.e., whether the determinant factor of application is operating aircrafts for remuneration or hire, and whether the provisions of this Proposal apply also to general aviation and/or private aviation. The Commission is invited to provide clarifications on that point.



Article 3 point (i): Article 4 (3a) of the Regulation [API Border] states that "The API data shall also consist of the following flight information relating to the flight of each traveller: the flight identification number or, if no such number exists, other clear and suitable means to identify the flight;". The relevant delegated acts or the practical handbook should describe cases in which no such number exists (e.g. carriers with no ICAO/IATA codes or carriers with no flight numbers, but flying using call signs), because the means for flight identification need to not contradict the current PIUs' practice. For example, regarding carriers with no ICAO/IATA codes, the usual practice of most PIUs is assigning a unique 3-char code to each of those carriers to be utilized for their transmissions. The issue should be noted and taken into consideration, since correlation (hence joint processing) of API and PNR data in most MSs PNR systems is achieved, to our knowledge, based primarily on that flight identification information.

General Note: This Proposal does not include any provisions regarding irregular operations (especially flights diversions and emergency landings, for which data still need to be transmitted to the PIUs).

CHAPTER 2: PROCESSING OF API DATA

Article 4 § 9: The Commission should take into consideration the supported data formats currently used for the transfers of API data, in order to avoid any unnecessary incurring development costs in the PIUs' system. Namely, in WK 3056/2023 INIT "*Working Party on JHA Information Exchange (IXIM) of 1-2 March 2023 - Presentations*", formats PAXLST UN/EDIFACT 15b and JSON/XML are noted. PAXLST UN/EDIFACT is mentioned in Implementing Decision (EU) 2017/759, while JSON/XML is not. Thus, Hellenic PIU welcomes the note made in the same document about the router being about to convert from JSON/XML to PAXLST 15b and then transmit the data to the PIUs. We believe that this general capability should be mentioned in written either in the Proposal or the relevant delegated act. In the latter case, this could be further analyzed during the preparation of delegated acts, mentioned in Recital 24.

<u>Article 5:</u> Our comments noted on Article 1 (c) also apply here. For those reasons, we propose deletion of the pre-latter sentence of Article 5 (1) "*However, for intra-EU flights, the router shall only transmit the API data to that PIU in respect of the flights included in the list referred to in paragraph 2.*" and of the whole Article 5 (2) "*Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. Those Member States shall, in accordance with Article 2 of that Directive, regularly review and where necessary update those lists and shall immediately provide eu-LISA with any such updated lists. The information contained on those lists shall be treated confidentially.*".

CHAPTER 3: LOGGING, PERSONAL DATA PROTECTION AND SECURITY

Article 7: We strongly believe that eu-LISA shall also be controller, within the meaning of Article 3, point (8) of Regulation (EU) 2018/1725, in relation to the processing of API data constituting personal data under this Proposal. Specifically, eu-LISA and the PIUs, shall act as joint controllers, in light of Article 28 of Regulation (EU) 2018/1725 and Article 21 of Directive (EU) 2016/680, in relation to the processing actions performed by them and in accordance with their responsibilities for compliance with their data protection obligations, which need to be further specified in a transparent manner in the Proposal, so that no arrangement between them is later deemed necessary.

The observation of not appointing eu-LISA as processor was also mentioned in a previous IXIM meeting by some countries, including Greece, with the response of the Commission being to recall Opinion 6/2023 of European Data Protection Supervisor (EDPS) that considered the designation of roles in the API Proposals appropriate (point 33).

Though, we kindly bring to your attention the following background:

- Opinion 06/2016 EDPS Opinion on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System: "*The EDPS understands that eu-LISA will be responsible for the security of the web service, the security of the personal data it contains and the process to get the personal data from the central system into the web service, and should thus be considered as controller as regards these issues. The EDPS recommends to clearly specify these responsibilities in the 2016 EES Proposal.*" (point 49).

- Opinion 03/2017 EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS): "*The EDPS recommends a more accurate description of the division of roles between the EBCG Agency and eu-LISA by considering, where appropriate, their designation as joint controllers.*" (point 87).

- Opinion 11/2017 EDPS Opinion on the proposal for a Regulation on ECRIS-TCN: "*The EDPS on several occasions has pointed to the implications of the distribution of roles amongst several actors in EU large scale databases and recommended that where an actor independently defines purposes or means of the data processing it should be considered controller rather than processor. Several actors thus contributing to the purposes and/or means of processing, as the case here is, should be considered joint controllers.*" (point 40).

- Opinion 4/2018 EDPS Opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems: "*As explained above, the concept of controllership is based on a factual analysis. The assignment of roles in the Proposal for a Regulation leads to a situation where Member States are responsible for matters not under their control (e.g. how eu-LISA manages information security and secure transmission of the data to and from the databases). Additionally, euLISA receives tasks (developing the system, ensuring its security during operations etc.) that according to the proposals, it is meant to fulfil with greater autonomy than that of a processor. Therefore, we recommend designating eu-LISA and the competent authorities of the Member States as joint controllers, each with their clearly defined tasks and responsibilities.*" (point 107).

- Opinion 9/2018 EDPS Opinion Proposal for a new Regulation on the Visa Information System: "Accordingly, eu-LISA would act as controller in the meaning of Article 3(8) of Regulation 2018/1725 and would have to implement appropriate technical and organisational measures to ensure the secure processing." (point 83).

Despite the above EDPS Opinions, eu-LISA was not assigned as controller in all Regulations that followed (EES, ETIAS, ECRIS-TCN, Interoperability Framework, VIS).

Moreover, our position for joint controllership of eu-LISA and PIUs is supported for the following reasons:

- The division of roles and responsibilities is vague and efforts should be taken to clearly delineate them in the Proposal.

- Article 6 (8) of the PNR Directive provides that "*The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States*". The Proposal provides that eu-LISA will be responsible for multiple actions that require processing of data, while these roles will be carried out in locations outside each MS's territory.

- While of course the purposes (and to a certain extent the means) of processing are defined in the Proposal, the controller is accountable for implementing appropriate technical and organizational measures to ensure that the processing is carried out in accordance with data protection rules, as well as should be able to demonstrate that this is the case. With the distribution of roles as included in the Proposal, PIUs could find itself in a position where they could be held accountable (as controllers) for matters being outside of the scope of their influence, as they are exclusively allocated to eu-LISA (namely receipt of incoming API data, data format verification, route identification, data tranfer verification, transmission of API data to the PIUs, deletion of API data for not selected intra-EU flights, access to data for maintenance reasons, storage of data for technical reasons).

- On the latter note, the EDPS mentions that there is no "true" storage of API data in the router, in an effort to provide arguments for the designation of eu-LISA as processor, instead of controller. At the same time, Article 7 clearly states: "*the PIUs shall be controllers, within the meaning of Article 3, point (8), of Directive (EU) 2016/680 in relation to the processing of API data constituting personal data under this Regulation through the router, including transmission and* ***storage for technical reasons of that data on the router***". The Commission is invited to comment on that point.

- Last but not least, **acceptance of the EDPS opinion characterizing all means related with the practical aspects of implementation as "non-essential**", hence left to be decided by eu-LISA as processor rather than controller, **logically entails that** since these means are not even determined by the PIUs acting as controllers, **the phrase "*including transmission and storage for technical reasons of that data on the router*" should be deleted from the competences of the PIUs in Article 7**.

Article 9: In case our comments for specific designation of PIUs' and eu-LISA's responsibilities as joint controllers are not to be accepted and taking into account that the PIUs will be designated as controllers, self-monitoring their compliance on the part of processing done by the eu-LISA would entail PIUs' direct access to the logs kept by eu-LISA, in accordance with Article 13 of API Border Proposal, but only the logs that each MS PIU is entitled to verify frequently (the ones that concern data for flights departing from/ landing on its territory). The Commission is invited to provide guidance on how that prerequisite of the PIUs' self-monitoring obligation set in this Article would be implemented.

Article 11 and 12: We believe that a specific reference should be include that the costs incurred by the air carriers, in relation to their connections to and integration with the router, administration, use and maintenance, shall be borne by them and not by the member states.

Article 13 par. 1: Insofar as the technical impossibility because of a failure of the router prevents the transfer of API data to it, the obligation for air carriers to transfer that API data to the router should **not** cease to apply.

A provision, similar to the one made in Presidency's compromise proposal for Regulation [API Border], instructing carriers to store the API data until the technical impossibility has been successfully addressed and at that point transfer the data to the router, **would be welcomed, yet would not still be considered adequate**.

Recital 21 states, inter alia, that "*given the unavailability of the router ... it will generally not be reasonably possible for air carriers to transfer the API data affected by the failure in a lawful, secure, effective and swift manner through alternative means*", while **this is not the case**.

Hellenic PiU, as well as many other MSs, has already established **separate secure direct connections** with carriers and providers, while, at the same time, has developed **a lawful, secure and effective dedicated web application, co-funded by European Union (ISF- Police),** in the context of implementing PNR Directive, to be utilized by carriers and providers for the transfer of their data to our database in cases of technical failure.

In this light, we strongly believe that a provision on **transfers through alternative means** should be included in this article, especially taking into account that, at this stage, **the time period, during which a possible technical failure to the router would persist, cannot be determined**.

The Commission is kindly invited to take that capability into deep consideration, bearing in mind that **the pursued purposes** of prevention, detection, investigation and prosecution of terrorist offences and serious crimes **can only be achieved by timely transmissions**. Moreover, already applicable solutions **developed utilizing European funds** will be rendered **inactive**.

Separately, we noticed that the Commission is not included in the notification recipients in this paragraph, in contradiction with the next two ones. If the Commission shares the position that it has to be informed in cases of failure of the router, also, we propose addition of it in the recipients' list.

Article 13 par. 2: Similarly, to our comments above, we believe that a provision for eu-LISA to store the API data until the technical impossibility has been successfully addressed and at that point transfer the data to the MS should be included, as well as a provision for transfers by the air carriers through alternative means directly to the MS experiencing the technical impossibility to utilize the router for as long as this failure persists.

Moreover, we do not see the reason why the air carriers should be apprised of such a failure, especially in case they are not requested to proceed to transfers through alternative means.

On that note, other PIUs also do not have any involvement in such a case, hence notifying them on the matter does not align with the "need-to-know" principle, which reflects the quintessence of our Unit's rules of procedure.

Last but not least, in order for the possibility of connection failure between eu-LISA and a MS to be limited, **we would be in favor of the establishment of primary and secondary connections between eu-LISA and all MSs.**

Article 13 par. 3: With the above in mind, we suggest that a provision for carriers to store the API data until the technical impossibility has been successfully addressed and at that point transfer the data to the router should be included, as well as a provision for the possibility of transfers by the air carriers through alternative means directly to the MS.

Additionally, in our view, the report containing all necessary details on the technical impossibility, including the reasons for the technical impossibility, its extent and consequences as well as the measures taken to address it, **should definitely be submitted to the PIUs** and (possibly) to the eu-LISA, apart from the competent national supervisory authority referred to in Article 15.

Article 17: Hellenic PiU welcomes the provision of the Commission preparing the practical handbook **in close cooperation with the PIUs**. We believe that our operational experience can prove rather beneficial in the making of the aforementioned handbook, as many matters that **have already been encountered and resolved by Hellenic PiU** would have to be taken into account.

SPAIN

Article 1

As already mentioned by this Delegation during the last IXIM meeting, it is requested to COM that paragraph 1a) be amended by deleting the word "selected", so that airlines do not have access to data on which flights are selected by the MS, due to fact that this information should only be known by the competent authorities of the MS. The airlines have to collect and send to the Router the data for all flights; the Router then will filter afterwards, as mentioned before.

On the other hand, about Article 1c), given that the nature of this Regulation is to prevent, detect and investigate acts of terrorism and other serious crimes (obtaining advanced information from passengers), ES suggests the possibility for the COM to study possible ways for the transmission of data from the Router, in certain situations given by exceptional circumstances, could also go simultaneously to the competent authorities dedicated to this type of serious crime, in addition to the PIU as stated in the Regulation. This would save time in the subsequent forwarding from the PIUs to them, avoiding delays in critical situations, as determined by the MS. The dynamics of preventive and investigative police activity, concerning the seriousness of the crimes concerned, make it essential for the investigative units of the competent authorities to react immediately.

Article 2

It is significant that in the API Borders proposal, all flight departs (scheduled and non-scheduled have been deleted) and in this one, the distinction is maintained.

Article 7

This Delegation proposes to clarify the article and to expressly mention the responsibility of eu-LISA in the article, proposing to reproduce what is already stipulated in the API Borders Regulation.

It is considered that EULISA should be listed as a "processor" in terms of its Router function, analogous to Article 16 of the API Borders. At the same time, both PIUs and airlines should be mentioned as "controllers".

Article 8

Comments by ES Delegation were already made within the security part of the API Borders proposal. It is about defining in more detail what is related to security, perhaps not in the articles, but through a delegated or implementing act (preferably an implementing act), with all the concrete details, as far as the security of the exchanges is concerned

Article 10

In line with the comment made concerning Article 1c), it is suggested that the COM could study the feasibility of establishing a tool/procedure/mechanism which, in situations of temporary need related to security (terrorism or serious crime), could establish an infrastructure that, at the national level, would allow the Router to send data to the competent authorities simultaneously with its transmission to the PIU.

Regarding the possible implications of including this referred mechanism in the API LEW Regulation, with the PNR Directive, such a Directive itself provides in art. 4(2)(a) as follows: “collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities referred to in Article 7”. Article 7 PNR states that each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU to examine that information further or to take appropriate action to prevent, detect, investigate and prosecute terrorist offences or serious crime.

Therefore, at a first glance, direct transmission of data from the Router to the competent authorities simultaneously to the PIU, in some particular and exceptional cases, would not mean a breach of the PNR Directive. Maybe it requires further in deep study.

Article 16

Here the ES Delegation presents a similar contribution to that made in the API Borders proposal. It concerns homogenisation, which has already been expressed. This Delegation is in favour of having maximum and minimum thresholds, and even that sanctions could be identical in all MS, to avoid the same company with a similar breach being sanctioned differently depending on the MS. For establishing the thresholds and guidelines could be sufficient to be included in an implementing act containing all details.

It is also advisable to propose non-financial sanctions, which could stand as far as temporary or permanent bans on airlines that systematically fail to comply across the EU, for instance, because it may be more profitable for them to fail to comply and pay penalties than to bear the costs of investment and data sending or for whichever other reasons.

Just to finalise, this Delegation has concerns that, for the time being, we don't found where to fit in the text, which is as follows: in the case of flights that have to make an emergency stopover (whatever the origin and destination is) and, therefore, not foreseen, the procedure for sending data should be included both in this API regulation and in the API Borders, considering it necessary for it to be sent from the router to the PIU.

FRANCE

NOTE DE COMMENTAIRES DES AUTORITES FRANCAISES

Objet: Note de commentaires suite à l'IXIM du 16-17 mars 2023 sur le règlement API 731 « Répressif » (chapitres I à VII – articles 1 à 21)

Réf.: COM (2022) 731 – Règlement API « Répressif »

<u>En remarques liminaires sur le transport aérien</u>

S'agissant du projet d'étendre l'obligation de collecte de données API sur les vols intra-Schengen, les autorités françaises souhaitent à nouveau interroger la Commission sur l'analyse d'impact de cette nouvelle mesure en termes de facilitation.

Après relecture de l'étude d'impact* élaborée par la Commission et en particulier de la partie mentionnée par la Commission lors de la dernière réunion, le sujet semble effectivement avoir été abordé (« *The collection of API data on intra-EU and domestic flights would also impact the check-in processes of airlines as, at present, the step of collecting data from identity cards or travel documents is not foreseen on these flights »**), mais l'impact de cette mesure ne semble pas avoir été pleinement appréhendé.

Afin de donner une idée du volume dont il est question : les vols Schengen de la compagnie Air France ont représenté en 2022 12,5 Millions de passagers dont il est estimé que 65% voyagent sans bagages. Ce sont donc plus de 8M de passagers qu'il conviendra de "traiter" pour collecter les données des passagers de cette seule compagnie.

Le fait que les passagers s'enregistrent en ligne comme l'évoque la Commission dans son étude d'impact ne permet pas de collecter les données API attendues, et tous les passagers ne passent pas aujourd'hui par une borne d'enregistrement. En revanche, demain, tous les passagers (sans bagages) devront impérativement s'arrêter à un point de leur parcours en aéroport afin que les données API soient collectées. Si cela était effectué à la porte d'embarquement (par exemple) cela aurait des conséquences potentiellement lourdes :

- pour les transporteurs, qui devront concilier cette collecte avec des temps de rotation appareils restreints (20 minutes pour certains opérateurs sur des vols intra Schengen)

- pour les aéroports, quelle que soit leur taille, qui devront éventuellement financer des infrastructures nouvelles (bornes ou autres dispositifs de collecte).

Dans ce contexte il est impératif que la Commission livre des éléments plus précis sur l'impact à venir ainsi que les moyens, techniques et opérationnels, envisagés pour alléger cette nouvelle contrainte. Qu'en est-il par exemple du « *digital travel certificate* » (DTC) ? Ce dispositif peut-il permettre d'atteindre l'objectif de fiabilisation des données API déclarées par le passager sans avoir forcément à les faire collecter en aéroport par le transporteur ?

**Etude d'impact*

Après vérification faite dans l'étude d'impact, et suite à la réponse de la Commission lors de la dernière réunion, le paragraphe auquel semble se référer la Commission dans son étude d'impact serait le suivant :

"Air industry would benefit from the capability of the API router to 'filter' the data and transmit it to competent authorities who would have direct access to the data instead of the individual system of the airline which may result in mistakes and loopholes. Therefore, a standardisation of the the data collection and transmission requirements is more efficient in ensuring correctness of the data and would significantly decrease the exposure to sanctions by Member States.

The collection of API data on intra-EU and domestic flights would also impact the check-in processes of airlines as, at present, the step of collecting data from identity cards or travel documents is not foreseen on these flights. *The increasing use of online check-ins was a means for the air industry to bring down the costs associated with the check-in. The measures proposed aim to strike a balance between these costs to collect API data from passengers while also ensuring high quality of the data transmitted, containing as few errors as possible and less exposition to sanctions from national authorities."*

Commentaires écrits sur le Règlement « Répressif » - COM (2022) 731 final

Considérant 15 :

Dans le considérant 15, les autorités françaises relèvent que le terme «*flight »* n'est pas correctement employé : "*the lists of the flights they selected,[...]"*. Les autorités françaises suggèrent de parler de ***route*** (aéroport de départ / aéroport d'arrivée). En effet, un vol est réalisé parce qu'il y a une route ouverte. Il peut y avoir sur une même route plusieurs vols de plusieurs compagnies avec des *PNR record locator* (code PNR unique) différents. De plus, un même avion peut être partagé par plusieurs compagnies sur une même route.

Aussi, le terme "*flight*" dans ce contexte des vols intra-UE pourra être modifié en "***route***" en référence à ce considérant dans l'ensemble du texte proposé. Les autorités françaises souhaitent donc que la confusion entre « vol(s) » et « route(s) » soit clarifiée et rappellent par la même leurs réserves sur l'aspect sélectif pour les vols intra-UE, vecteurs de criminalité importants.

Chapitre I : Dispositions générales

Article 1 : Objet

Les autorités françaises rappellent leur position consistant pour le moment à demander une étude d'impact d'extension au maritime (voire au ferroviaire, ce dernier ayant été évoqué par la Commission lors du groupe IXIM du 3 avril). La position de la France en faveur de cette extension sera confirmée au regard des résultats de cette étude d'impact, tant sur l'intérêt d'une telle extension que sur son impact sur les opérateurs.

Ce règlement régit uniquement la collecte et le transfert des données API par les transporteurs et ne mentionne pas le traitement ultérieur de ces données. Seul le considérant 5 mentionne les règles applicables au traitement des données, qui est régi par la directive PNR de 2016. Les autorités françaises proposent de clarifier les relations entre les deux textes dans le corps du règlement 731 avec l'ajout du paragraphe suivant : « ***The subsequent processing of data, collected and transmitted to PIUs under this regulation, shall be done in accordance with the rules set out in directive 2016/681*** ».

Les autorités françaises proposent de modifier la phrase de cet article pour éviter de laisser croire que ce sont les compagnies qui sélectionneront les routes intra-UE avec :

- au « a) » le retrait du terme « *selected* » devant intra-EU puisque la sélection des données des vols intra-UE ne doit pas être effectuée par les compagnies aériennes mais par le routeur. Les compagnies devront fournir l'entièreté des données au routeur.

- au (c) « *and selected intra UE flights /* ***routes by Member States according their operational needs*** »

Enfin, les autorités françaises rappellent que le présent règlement n'a pas vocation à s'appliquer aux activités qui relèvent de la seule compétence des Etats membres, comme les finalités de sécurité nationale, en application de l'article 4.2 TUE. Elles estiment que le considérant ne répond pas suffisamment à ce besoin, dans la mesure où il ne concerne que la collecte des données API pour d'autres modes de transport que le vecteur aérien. Elles souhaitent ainsi ajouter à l'article 1er une clause d'exclusion (comme il en existe une dans d'autres textes, comme par exemple, dans l'orientation générale du Conseil sur le règlement *ePrivacy*). La rédaction proposée est la suivante :

"This Regulation does not apply to activities which fall outside the scope of Union law, and in any event measures, shall not affect the possibility for Member States to provide, under their national law, for a system processing API data for the purpose of safeguarding national security'' ".

Enfin, il semble important aux autorités françaises que le terme "*flight*" soit remplacé par le terme « *route* » (remarque considérant 15) pour les vols extra et intra-UE.

Article 2 : Périmètre

Les autorités françaises n'ont pas de commentaire sur cet article.

Article 3 : Définitions

Les autorités françaises ont relevé plusieurs erreurs dans cet article :

(g) – « *crew* », il s'agirait de mentionner l'article 3 pt (i) du règlement Frontières au lieu du point (h).

(h) – « *traveller* », il s'agirait de mentionner l'article 3 pt (j) du règlement frontières au lieu du point (i)

(i) – « *advance passenger information* » - il s'agirait de mentionner l'article 3 pt (k) du règlement frontières au lieu du point (j)

(n) – « *the router* », il s'agirait de mentionner l'article 3 (m) du règlement frontières au lieu du (k).

Chapitre II : Traitement des données API

Article 4 : Collecte, transfert et suppression des données API par les transporteurs aériens

De manière générale, les autorités françaises souhaitent que les références au paragraphe soient explicitées :

§1 – Dans le détail, la phrase relative à la responsabilité du transfert des données par la compagnie opérant le vol si celui-ci est exploité par plusieurs compagnies n'apparaissait pas dans le règlement « frontières ». Les autorités françaises souhaitent savoir si cela se justifie par le fait que les vols extra-UE ne peuvent pas être exploités par plusieurs compagnies ? Dans ce cas, les autorités françaises suggèrent d'ajouter cette phrase présente dans le règlement « prévention/répression » dans le dispositif du règlement « frontières ».

§7 – Les autorités françaises proposent l'ajout suivant: *« and it is no longer possible for travellers to board or leave the aircraft and* ***for items to be added or removed*** *».*

§8 – (Paragraphe après le (b)) : à l'image du texte API Frontières, les autorités françaises s'interrogent sur la nécessité pour les transporteurs aériens d'informer eu-Lisa du transfert complet des données, qui doit ensuite informer les UIP de la réception des données par l'agence via le routeur (quel est le besoin sous-jacent ?)

Article 5 : Transmission des données API du routeur via les UIP

§2 – Ce paragraphe tient compte des exigences posées par le CJUE dans l'arrêt « Ligue des droits humains » qui oblige les États-membres à sélectionner des vols intra-UE en l'absence de démonstration d'une menace terroriste réelle et actuelle ou prévisible. Cependant, là où dans l'arrêt de la Cour on comprend qu'il sera possible d'éviter de sélectionner des routes si la menace réelle et actuelle ou prévisible est démontrée, il n'est rien prévu de similaire dans ce règlement API. Pour les autorités françaises, il est indispensable d'introduire une clause spécifique relative au cas de menace terroriste réelle, actuelle et prévisible qui permettrait de disposer de l'ensemble des vols intra-UE sur une période donnée. La Commission lors de la réunion IXIM a semblé indiquer que cette logique relative aux données PNR pouvait être appliquée aux données API lorsqu'elle a répondu à une question de la Belgique. Aussi, les autorités françaises souhaiteraient qu'une disposition sur ce point soit introduite dans le texte à l'article 5.

Enfin, concernant le caractère confidentiel du traitement, les autorités françaises se questionnent sur les modalités pratiques, dans la mesure où à notre connaissance, eu-LISA ne dispose pas d'un réseau sécurisé au niveau « confidentiel/secret » à ce jour.

Par ailleurs, il conviendrait de remplacer "*intra-UE flights*" par *'intra-UE routes*" (même remarque que le considérant 15).

Sur la proposition de la Slovaquie relative à l'accès par les Etats membres à la liste des vols intra-européens sélectionnés, pour les autorités françaises, il est envisageable et pourrait être utile de disposer d'informations sur les vols sélectionnés par les autres États membres. Cependant, ces listes et informations devront être protégées afin de ne pas être accessibles aux criminels et terroristes. Par ailleurs, les échanges d'informations entre les États membres devront se faire par des canaux sécurisés et adaptés. À notre connaissance, à ce jour il n'existe pas de canal idéal qui permettrait des échanges sécurisés d'informations devant être classifiées.

Chapitre III : Enregistrement, protection des données personnelles et sécurité

Article 6 : Conservation des registres (« logs »)

Les autorités françaises n'ont pas de commentaire sur cet article.

Article 7 : Contrôleurs des données personnes

Il est indiqué que les UIPs doivent être responsables de traitement des données API puisqu'elles constituent des données à caractère personnel (application du RGPD) au titre du règlement, par l'intermédiaire du routeur y compris pour la transmission et le stockage pour des raisons techniques, de ces données sur le routeur. Cependant il semblait que le routeur servirait davantage hub et ne devrait pas stocker, en tant que tel, les données. Les autorités françaises s'interrogent donc sur le sens de cet article.

Article 8 : Sécurité

Les autorités françaises s'interrogent sur les règles applicables en cas de transfert ultérieur vers des tiers et une potentielle référence explicite à la Directive Police-Justice dans ce chapitre et proposent l'ajout suivant : *« The PIUs shall ensure that API data are processed in accordance with the rules set out in directive 2016/680 and with the rules set out in directive 2016/681 in regards to transfers to third countries* ».

Article 9 : Autocontrôle

Les autorités françaises notent une erreur de mention, il devrait être fait référence à l'article 6 relatif aux logs et non à l'article 7.

Chapitre IV : Sujets concernant le routeur

Article 10 : Connexions des UIP au routeur

§1 – Il est indiqué : « *They shall ensure that their national systems and infrastructure for the reception and further processing of API data transferred pursuant to this Regulation are integrated with the router*".

Les autorités françaises souhaitent avoir des précisions quant à cette formule :

1. Les systèmes nationaux devront-ils s'insérer dans le routeur ?

2. Est-ce aux systèmes nationaux de s'adapter au routeur (cela ne devrait-il pas être l'inverse, le routeur étant créé de toutes pièces) ?

3. Par ailleurs quel type de communication est visé quand il est fait mention d'échanges d'informations liées aux transferts de données API (est-il question d'échanges d'informations entre UIPs ou plutôt entre les UIPs et le routeur) ?

Pour la deuxième partie du **§1,** les autorités françaises suggèrent la proposition rédactionnelle suivante : *"Member States shall ensure that the connection to that router and integration with it enables their PIUs to receive and further process the API data, as well* ***as to exchange any communications relating thereto****, in a lawful, secure, effective and swift manner."*

Article 11 : Connexions des transporteurs aériens au routeur

§1 – Les autorités françaises s'interrogent sur l'emploi du terme « *communication* » dans la mention *« as well as to exchange any **communications** relating thereto »* relatif aux transferts de données API des compagnies vers le routeur.

D'abord, les autorités françaises souhaitent interroger la Commission sur le sens du terme « ***communications*** ». Ensuite, le routeur ne risque-t-il pas d'être incapable de gérer des données/informations qui ne seraient pas des données API ?

Article 12 : Coût pour les Etats membres

Afin d'éviter une déperdition des budgets nationaux alloués aux Etats membres dans le cadre du Fonds de Sécurité Intérieure au vue des dépenses additionnelles liées au routeur, il faudrait prévoir un alinéa supplémentaire ajoutant un alinéa 3 à l'article 12:

Article 12

1. Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union.
However, the following costs shall be excluded and be borne by the Member States:

(a) cost for project management, including costs for meetings, missions and offices ;

(b) costs for the hosting of national information technology (IT) systems, including costs for space, implementation, electricity and cooling;

(c) costs for the operation of national IT systems, including operators and support contracts;
(d) costs for the design, development, implementation, operation and maintenanceof national communication networks.

2. Member States shall also bear the costs arising from the administration, use and maintenance of their connections to and integration with the router.

*3. **Funding to be mobilised from the envelope referred to in point (b) of Article 7(2) of Regulation (EU) No 2021/1149 to cover the costs of implementation of this Regulation referred to in paragraphs 1 to 2 of this Article shall be implemented under shared management. »***

Article 13 : Actions en cas d'impossibilité technique d'utilisation du routeur

Comme pour le règlement « Frontières », les autorités françaises estiment qu'il serait utile de disposer de plus de précisions sur l'existence d'un dispositif de secours et son fonctionnement. Une procédure alternative en cas de défaillance technique du routeur devrait être proposée pour limiter tout risque de faille. Rien n'est prévu comme alternative en cas de dysfonctionnement du routeur, outre la notification aux autorités et aux transporteurs par l'Agence eu-LISA.

Les autorités françaises déplorent qu'aucune procédure de secours concrète ne soit explicitée. Que deviennent les données API et comment les UIPs les recevront-ils en cas d'interruption prolongée sur le routeur ?

En outre, les autorités françaises renvoient à l'article 4 point 1 qui prévoit que les transporteurs aériens collectent les données API dans le but de les transmettre au routeur central. Il est logique que cette obligation de transfert des données au routeur ne s'applique pas lorsque ce dernier est en panne.

Cependant, les autorités françaises estiment qu'il conviendrait qu'en cas de panne du routeur les transporteurs aériens continuent de collecter les données API et les conservent. Par conséquent, les autorités françaises souhaitent que des précisions techniques (notamment pour la durée et lieu de conservation des données) soient explicitées dans cet article. Selon notre analyse, cette conservation des données pourraient être assurée soit par le transporteur (1), soit dans l'interface (2) par laquelle les transporteurs passent pour que les données soient ensuite envoyées vers le routeur. Les autorités françaises souhaitent connaître l'option privilégiée.

En conclusion, il semble crucial aux autorités françaises de renforcer à la fois la collecte et le transfert des données en cas de défaillance technique du routeur et, par conséquent, de prévoir d'autres canaux de transmission en cas d'impossibilité technique du routeur. En effet, les autorités françaises rappellent qu'une absence de collecte des données API en cas de panne du routeur poserait des difficultés pour les services répressifs qui ne disposeront dès lors plus de données essentielles à leurs enquêtes.

Article 14 : Responsabilité concernant le routeur

Les autorités françaises n'ont pas de commentaire sur cet article.

Chapitre V : Supervision, sanctions et manuel

Article 15 : Autorité de supervision nationale

Les autorités françaises n'ont pas de commentaire sur cet article.

Article 16 : Sanctions

Pour les autorités françaises, les sanctions devraient pouvoir être harmonisées au niveau européen pour éviter de trop grandes divergences entre les pratiques de chaque Etat membre (au sein d'un acte d'exécution ou, comme mentionné par la Commission, au sein du manuel pratique). Ces sanctions devraient également revêtir un caractère suffisamment « dissuasif ».

Article 17 : Manuel pratique

Les autorités françaises n'ont pas de commentaire sur cet article.

Chapitre VI : Relations avec les autres instruments existants

Article 18 : Amendements au règlement (UE) 2019/818

Les autorités françaises n'ont pas de commentaire sur cet article.

Chapitre VII : Dispositions finales

Les autorités françaises souhaitent privilégier le recours aux actes d'exécution pour les articles qui ne concernent/n'impliquent pas les transporteurs et proposent, en conséquence, d'ajouter un article régissant la procédure à suivre pour prendre des actes d'exécution.

Ajout d'un article 18 bis - *Committee procedure*

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), the third subparagraph, of Regulation (EU) No 182/2011 shall apply.

Article 19 : Exercice de la délégation

Les autorités françaises n'ont pas de commentaire sur cet article.

Article 20 : Surveillance et évaluation

Les autorités françaises n'ont pas de commentaire sur cet article.

Article 21 : Mise en œuvre et application

Les autorités françaises n'ont pas de commentaire sur cet article.

Points divers :

La Commission (soutenue par Irlande) a indiqué que les Etats membres ne participant pas à l'acquis Schengen ne seraient pas tenus de fournir les données API des vols entrants et sortants de leur territoire aux fins de contrôles aux frontières. Elle a également souhaité que les Etats membres fassent part de leur avis et besoins opérationnels en la matière. A cet égard, les autorités françaises rappellent que les données de ces pays sont particulièrement utiles pour les services opérationnels, en particulier en matière de trafic d'armes, de proxénétisme et de renseignement criminel.

Courtesy translation

Introductory remarks on air transportation

With regard to the plan to extend the obligation to collect API data on intra-Schengen flights, the French authorities would like to ask the Commission once again about the impact analysis of this new measure in terms of facilitation.

After rereading the impact study* prepared by the Commission, and in particular the part mentioned by the Commission at the last meeting, the subject seems to have been addressed ("*The collection of API data on intra-EU and domestic flights would also impact the check-in processes of airlines as, at present, the step of collecting data from identity cards or travel documents is not foreseen on these flights* "*), but the impact of this measure does not seem to have been fully apprehended.

To give an idea of the volume involved: Air France's Schengen flights represented 12.5 million passengers in 2022, of which it is estimated that 65% travel without baggage. Therefore, more than 8 million passengers will have to be "processed" in order to collect passenger data from this airline alone.

The fact that passengers check in online, as mentioned by the Commission in its impact study, does not allow for the collection of the expected API data, and not all passengers today go through a check-in kiosk. On the other hand, tomorrow, all passengers (without baggage) will have to stop at some point in their journey through the airport in order for API data to be collected. If this were done at the gate (for example), it would have potentially serious consequences:

- for carriers, who would have to reconcile this collection of data with restricted aircraft turnaround times (20 minutes for some operators on intra-Schengen flights)

- for airports, whatever their size, which may have to finance new infrastructure (terminals or other collection systems).

In this context, it is imperative that the Commission provide more precise information on the future impact and the technical and operational means envisaged to alleviate this new constraint. What about the "*digital travel certificate*" (DTC), for example? Can this system achieve the objective of making the API data declared by the passenger more reliable without necessarily having to have it collected at the airport by the carrier?

**Impact Study*

After checking the impact statement, and following the Commission's response at the last meeting, the paragraph to which the Commission seems to be referring in its impact statement would be the following:

"The airline industry would benefit from the API router's ability to 'filter' data and pass it to the appropriate authorities who would have direct access to the data instead of the individual airline's system which can lead to errors and gaps. Therefore, standardization of data collection and transmission requirements is more effective in ensuring data accuracy and would significantly reduce the risk of sanctions from member states.

The collection of API data on intra-Community and domestic flights would also have an impact on airline check-in procedures because there are currently no plans to collect data from ID cards or travel documents on these flights*. The increasing use of online check-in was a way for the airline industry to reduce the costs associated with check-in. The proposed measures aim to strike a balance between these costs of collecting API data from passengers while ensuring a high quality of the data transmitted, containing as few errors as possible and less exposure to sanctions from national authorities."*

Written comments on the "Law Enforcement" Regulation - COM (2022) 731 final

Recital 15:

In recital 15, the French authorities note that the term "flight" is not used correctly: "the lists of the flights they selected [...]". The French authorities suggest that the term "route/itinerary" should be used (airport of departure / airport of arrival). Indeed, a flight is made because there is an open route. There can be several flights of several companies with different PNR record locators (unique PNR code) on the same route. In addition, the same aircraft can be shared by several companies on the same route.

Therefore, the term "flight" in the context of intra-EU flights could be changed to "route/itinerary" in reference to this recital throughout the proposed text. The French authorities would therefore like the confusion between "flight(s)" and "route(s)" to be clarified and would like to reiterate their reservations about the selective aspect for intra-EU flights, which are major vectors of crime.

Chapter I

Article 1

The French authorities reiterate their position, which for the moment consists of requesting an impact study on the extension to maritime transport (or even to rail transport, the latter having been mentioned by the Commission at the IXIM meeting on 3 April). France's position in favour of this extension will be confirmed in light of the results of this impact study, both on the interest of such an extension and on its impact on operators.

This regulation only governs the collection and transfer of API data by carriers and does not mention the further processing of these data. Only Recital 5 mentions the rules applicable to data processing, which is governed by the 2016 PNR Directive. The French authorities propose to clarify the relationship between the two texts in the body of Regulation 731 with the addition of the following paragraph: "***The subsequent processing of data, collected and transmitted to PIUs under this regulation, shall be done in accordance with the rules set out in Directive 2016/681***".

The French authorities propose to modify the sentence of this article to avoid giving the impression that it is the companies that will select the intra-EU routes:

- in "(a)" the removal of the word "selected" in front of intra-EU since the selection of data for intra-EU flights should not be done by the airlines but by the router. The airlines will have to provide the router with all the data.

- in "(c)" adding the following: "*and selected intra EU flights / **routes by Member States according to their operational needs**"*

Finally, the French authorities point out that this regulation is not intended to apply to activities that fall within the sole competence of the Member States, such as national security purposes, pursuant to Article 4.2 of the EU Treaty. They consider that the recital does not sufficiently meet this need, insofar as it only concerns the collection of API data for modes of transport other than air transport. They therefore wish to add an exclusion clause to Article 1 (as exists in other texts, such as the Council's general approach on the e-Privacy Regulation). The proposed wording is as follows:

"This Regulation does not apply to activities which fall outside the scope of Union law, and in any event measures, shall not affect the possibility for Member States to provide, under their national law, for a system processing API data for the purpose of safeguarding national security".

Finally, it seems important to the French authorities that the term "flight" be replaced by the term "route" (see recital 15) for extra and intra-EU flights.

Article 2

The French authorities have no comment on this article.

Article 3

The French authorities have noted several errors in this article:

(g) - "crew", Article 3 point (i) of the Frontiers Regulation should be mentioned instead of point (h).

(h) - "traveller", it should refer to article 3 point (j) of the border regulation instead of point (i)

(i) - "advance passenger information" - this would mean referring to Article 3 point (k) of the Frontier Regulation instead of point (j)

(n) - "the router" - this would mean referring to article 3 (m) of the border regulation instead of (k).

Chapter II

Article 4

In general, the French authorities would like the references in the paragraph to be clarified:

§1 - In detail, the sentence relating to the responsibility for the transfer of data by the company operating the flight if it is operated by several companies does not appear in the "borders" regulation. The French authorities would like to know whether this is justified by the fact that extra-EU flights cannot be operated by several companies. If so, the French authorities suggest adding this sentence, which is present in the "law enforcement" regulation, to the provisions of the "borders" regulation.

§7 - The French authorities propose the following addition: "***and it is no longer possible for travellers to board or leave the aircraft and for items to be added or removed***".

§8 - (Paragraph after (b)): like the API borders text, the French authorities question the need for air carriers to inform eu-Lisa of the complete transfer of data, which must then inform the PIUs of the receipt of the data by the agency via the router (what is the underlying need?)

Article 5

§2 - This paragraph takes into account the requirements set by the CJEU in the "*Ligue des droits humains*" judgment, which obliges Member States to select intra-EU flights in the absence of a demonstration of a real and present or foreseeable terrorist threat. However, whereas the Court's ruling states that it will be possible to avoid selecting routes if a real and present or foreseeable threat is demonstrated, nothing similar is provided for in this API regulation. For the French authorities, it is essential to introduce a specific clause relating to the case of a real, current and foreseeable terrorist threat, which would make it possible to have all intra-EU flights available over a given period. During the IXIM meeting, the Commission seemed to indicate that this logic regarding PNR data could be applied to API data when it answered a question from Belgium. The French authorities would therefore like to see a provision on this point introduced into the text in Article 5.

Finally, concerning the confidential nature of the processing, the French authorities wonder about the practical arrangements, insofar as, to our knowledge, eu-LISA does not yet have a secure network at the "confidential/secret" level.

Furthermore, "intra-EU flights" should be replaced by "intra-EU routes" (same remark as in recital 15).

With regard to the proposal by Slovakia concerning access by the Member States to the list of selected intra-European flights, for the French authorities, it is conceivable and could be useful to have information on the flights selected by the other Member States. However, these lists and information will have to be protected so as not to be accessible to criminals and terrorists. Furthermore, the exchange of information between Member States will have to be done through secure and appropriate channels. To our knowledge, to date there is no ideal channel that would allow for the secure exchange of information that must be classified.

Chapter III

Article 6

The French authorities have no comment on this article.

Article 7

It is stated that PIUs must be responsible for the processing of API data since it constitutes personal data (application of the GDPR) under the regulation, through the router, including for the transmission and storage for technical reasons, of this data on the router. However, it seemed that the router would serve more as a hub and should not store, as such, the data. The French authorities therefore question the meaning of this article.

Article 8

The French authorities question the rules applicable in the event of subsequent transfers to third parties and a potential explicit reference to the Police-Justice Directive in this chapter and propose the following addition: ***"The PIUs shall ensure that API data are processed in accordance with the rules set out in directive 2016/680 and with the rules set out in directive 2016/681 with regard to transfers to third countries"***.

Article 9

The French authorities note an error in the reference, it should refer to Article 6 on logs and not to Article 7.

Chapter IV

Article 10

§1 - It is stated: "*They shall ensure that their national systems and infrastructure for the reception and further processing of API data transferred pursuant to this Regulation are integrated with the router*".

The French authorities would like to have clarification on this formula:

1. Will the national systems have to be integrated with the router?

2. Is it up to the national systems to adapt to the router (shouldn't it be the other way around, the router being created from scratch)?

3. Moreover, what type of communication is meant when mentioning information exchanges related to API data transfers (is it information exchanges between PIUs or rather between PIUs and the router)?

For the second part of §1, the French authorities suggest the following wording: "*Member States shall ensure that the connection to that router and integration with it enables their PIUs to receive and further process the API data,* ***as well as to exchange any communications relating thereto****, in a lawful, secure, effective and swift manner."*

Article 11

§1 - The French authorities question the use of the term "*communication*" in the phrase "*as well as to exchange any communications relating thereto*" in relation to the transfer of API data from the companies to the router.

First, the French authorities wish to question the Commission on the meaning of the term "*communications*". Second, is there not a risk that the router will be unable to manage data/information that is not API data?

Article 12

In order to avoid a loss of national budgets allocated to the Member States within the framework of the Internal Security Fund in view of the additional expenses related to the router, an additional paragraph should be added to Article 12:

Article 12
1. Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union.
However, the following costs shall be excluded and be borne by the Member States:

(a) cost for project management, including costs for meetings, missions and offices ;

(b) costs for the hosting of national information technology (IT) systems, including costs for space, implementation, electricity and cooling;

(c) costs for the operation of national IT systems, including operators and support contracts;
(d) costs for the design, development, implementation, operation and maintenanceof national communication networks.

2. Member States shall also bear the costs arising from the administration, use and maintenance of their connections to and integration with the router.

3. Funding to be mobilised from the envelope referred to in point (b) of Article 7(2) of Regulation (EU) No 2021/1149 to cover the costs of implementation of this Regulation referred to in paragraphs 1 to 2 of this Article shall be implemented under shared management. »

Article 13: Actions in the event of technical impossibility of using the router

As in the case of the "borders" regulation, the French authorities believe that it would be useful to have more details on the existence of a backup system and its operation. An alternative procedure in case of technical failure of the router should be proposed to limit any risk of failure. There is no provision for an alternative procedure in the event of router malfunction, other than notification of the authorities and carriers by the eu-LISA Agency.

The French authorities deplore the fact that no concrete backup procedure is spelled out. What happens to the API data and how will the PIUs receive it in the event of a prolonged interruption on the router?

In addition, the French authorities refer to Article 4 point 1, which provides that air carriers shall collect API data in order to transmit them to the central router. It is logical that this obligation to transfer data to the router does not apply when the router is down.

However, the French authorities consider that it would be appropriate for air carriers to continue to collect and retain API data in the event of a router failure. Consequently, the French authorities would like technical details (in particular the duration and location of data retention) to be clarified in this article. According to our analysis, this data storage could be ensured either by the carrier (1) or in the interface (2) through which the carriers pass so that the data are then sent to the router. The French authorities would like to know which option is preferred.

In conclusion, it seems crucial to the French authorities to strengthen both the collection and transfer of data in the event of technical failure of the router and, consequently, to provide for other transmission channels in the event of technical impossibility of the router. Indeed, the French authorities point out that a lack of API data collection in the event of router failure would pose difficulties for law enforcement agencies, which would then no longer have access to data essential to their investigations.

Article 14

The French authorities have no comment on this article.

Chapter V

Article 15

The French authorities have no comments on this article.

Article 16

For the French authorities, it should be possible to harmonize sanctions at the European level in order to avoid excessive divergence between the practices of each Member State (in an implementing act or, as mentioned by the Commission, in the practical manual). These penalties should also be sufficiently "dissuasive".

Article 17

The French authorities have no comments on this article.

Chapter VI

Article 18

The French authorities have no comments on this article.

Chapter VII

The French authorities wish to give preference to the use of implementing acts for articles that do not concern/involve carriers and therefore propose to add an article governing the procedure to be followed for taking implementing acts.

Addition of an article 18 bis - Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), the third subparagraph, of Regulation (EU) No 182/2011 shall apply.

Article 19

The French authorities have no comments on this article.

Article 20

The French authorities have no comments on this article.

Article 21

The French authorities have no comments on this article.

Other items:

The Commission (supported by Ireland) indicated that Member States not participating in the Schengen acquis would not be required to provide API data on flights entering and leaving their territory for the purposes of border controls. It also wanted the Member States to share their opinions and operational needs in this area. In this respect, the French authorities recall that the data from these countries is particularly useful for operational services, especially in the areas of arms trafficking, pimping and criminal intelligence.

ITALY

MODULARIO Interno - 372

Mod. 36/4 *PSC*

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

DIREZIONE CENTRALE DELLA POLIZIA CRIMINALE

Servizio per la Cooperazione Internazionale di Polizia
Delegazione IXIM

MI-123-U-B-IXIM-2023-51 Roma, 5th of April 2023

SUBJECT: IXIM – API Law Enforcement Authorities - Proposal COM(2022) 731.
Italian contribution.

TO IXIM WP

Bruxelles (BE)

With reference to the API LEAs' proposal, the Italian delegation wishes to submit to the attention of the Presidency and the IXIM Delegations the attached document containing the Italian amendments to the proposal as above in order to have a more powerful instrument for tackling terrorist offences and serious crimes.

The Italian proposal aims to:

- allow the MS to retain data on all extra-EU flights and intra-EU flights for up to a maximum of 3 years, in order to provide the competent national Authorities with an extremely important information asset to be used for investigative purposes only;
- enable the MS to carry out preventive cross checks for national security purposes against API data of extra-EU and selected intra-EU flights (according to the Court's ruling on PNR Directive).

To this regard, we consider essential to introduce the following principles:

1) removal of the obligation for MS to notify eu-LISA about the selected routes;
2) transmission by the router of all intra-EU flight data[2];
3) explicit provision of a right to retain all intra-EU flight data for a period of maximum 3 years, to be accessed only for judicial or investigation purposes;
4) provision of specific safeguards (depersonalized data) to limit the access to stored data unless being justified by concrete investigation purposes (e.g. by requesting a judicial authorization);
5) introduction of a specific power for MS to conduct preventive cross-checks against both API data of extra-EU flights and intra-EU flights selected on the basis of the risk assessment conducted at national level. The PIU will carry out such checks only once and upon receipt of such data.

We remain available for any further details on the matter and apologize for the late submission.

e-signed by
the head of IXIM delegation
Federico Sciaudone

[2] Points nr. 1 and 2 are the core of the proposal, since they allow MS to receive all the intra-EU flights API data.

HAVE ADOPTED THIS REGULATION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes, this Regulation lays down the rules on:

(a) the collection by air carriers of advance passenger information data ('API data') on extra EU flights and intra EU flights;

(b) the transfer by air carriers to the router of the API data;

(c) the transmission from the router to the Passenger Information Units ('PIUs') of the API data on extra-EU flights and intra-EU flights;

(d) the treatment of the API data on extra-EU flights and intra-UE flights by the PIU and the competent National Authorities.

Article 2

Scope

This Regulation applies to air carriers conducting scheduled or non-scheduled extra-EU flights or intra-EU flights.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(a) ‘air carrier’ means an air transport undertaking as defined in Article 3, point (1), of Directive (EU) 2016/681;

(b) ‘extra-EU flights’ means any flight as defined in Article 3, point (2), of Directive (EU) 2016/681;

(c) ‘intra-EU flight’ means any flight as defined in Article 3, point (3), of Directive (EU) 2016/681;

(d) ‘scheduled flight’ means a flight as defined in Article 3, point (e), of Regulation (EU) [API border management];

(e) ‘non-scheduled flight’ means a flight as defined in Article 3, point (f), of Regulation (EU) [API border management];

(f) ‘route’ means the itinerary made by scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop overs in the territory of a third country;

(g) ‘passenger’ means any person as defined in Article 3, point (4), of Directive (EU) 2016/681;

(h) ‘crew’ means any person as defined in Article 3, point (h), of Regulation (EU) [API border management];

(i) ‘traveller’ means any person as defined in Article 3, point (i), of Regulation (EU) [API border management];

(j) ‘advance passenger information data’ or ‘API data’ means the data as defined in Article 3, point (j), of Regulation (EU) [API border management];

(k) ‘passenger name record’ or 'PNR' means a record of each passenger’s travel requirements as defined in Article 3, point (5), of Directive (EU) 2016/681;

(l) ‘Passenger Information Unit’ or ‘PIU’ means the competent authority established by a Member State, as contained in the notifications and modifications published by the Commission pursuant to Article 4(1) and (5), respectively, of Directive (EU) 2016/681;

(m) ‘terrorist offences’ means the offences as defined in Articles 3 to 12 of Directive (EU) 2017/541 of the European Parliament and the Council[1];

(n) ‘serious crime’ means the offences as defined in Article 3, point (9), of Directive 2016/681;

(o) ‘the router’ means the router as defined in Article 3, point (k) of Regulation (EU) [API border management];

(p) ’personal data’ means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(q) ‘National Authorities’ means the National Authorities as defined in Article 7, point (1) and (2), of Directive (EU) 2016/681

[1] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

CHAPTER 2

PROCESSING OF API DATA

Article 4

Collection, transfer and deletion of API data by air carriers

1. Air carriers shall collect API data of travellers on the flights referred to in Article 2, for the purpose of transferring that API data to the router in accordance with paragraph 6. Where the flight is code-shared between one or more air carriers, the obligation to transfer the API data shall be on the air carrier that operates the flight.

2. Air carriers shall collect the API data in such a manner that the API data that they transfer in accordance with paragraph 6 is accurate, complete and up-to-date.

3. Air carriers shall collect the API data referred to Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means to collect the machine-readable data of the travel document of the traveller concerned. They shall do so in accordance with the detailed technical requirements and operational rules referred paragraph 5, where such rules have been adopted and are applicable.

   However, where such use of automated means is not possible due to the travel document not containing machine-readable data, air carriers shall collect that data manually, in such a manner as to ensure compliance with paragraph 2.

4. Any automated means used by air carriers to collect API data under this Regulation shall be reliable, secure and up-to-date.

5. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down detailed technical requirements and operational rules for the collection of the API data referred to in Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means in accordance with paragraphs 3 and 4 of this Article.

6. Air carriers shall transfer the API data collected pursuant to paragraph 1 to the router, by electronic means. They shall do so in accordance with the detailed rules referred to in paragraph 9, where such rules have been adopted and are applicable.

7. Air carriers shall transfer the API data both at the moment of check-in and immediately after the travellers have boarded the aircraft and it is no longer possible for travellers to leave the aircraft.

8. Without prejudice to the possibility for air carriers to retain and use the data where necessary for the normal course of their business in compliance with the applicable law, air carriers shall immediately either correct, complete or update, or permanently delete, the API data concerned in both of the following situations:

   (a) where they become aware that the API data collected is inaccurate, incomplete or no longer up-to-date or was processed unlawfully, or that the data transferred does not constitute API data;

   (b) where the transfer of the API data in accordance with paragraph 3 has been completed.

   Where the air carriers obtain the awareness referred to in point (a) of the first subparagraph of this paragraph after having completed the transfer of the data in accordance with paragraph 6, they shall immediately inform the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). Upon receiving such information, eu-LISA shall immediately inform the PIUs that received the API data transmitted through the router.

9. The Commission is empowered to adopt implementing acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of API data to the router referred to in paragraph 6.

Article 5

Transmission of API data from the router to the PIUs

1. The router shall immediately and in an automated manner, transmit the API data, transferred to it by air carriers pursuant to Article 4, to the PIUs of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, or to both in the case of intra-EU-flights. Where a flight has one or more stop-overs at the territory of other Member States than the one from which it departed, the router shall transmit the API data to the PIUs of all the Member States concerned.

   For the purpose of such transmission, eu-LISA shall establish and keep up-to-date a table of correspondence between the different airports of origin and destination and the countries to which they belong

The router shall transmit the API data in accordance with the detailed rules referred to in paragraph 3, where such rules have been adopted...

3. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

Article 5a

Treatment of API data by the PIU

1. Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of selected intra-EU flights as result of a domestic risk assessment.

   For the purpose of preventing the commission of terrorist offences or serious crimes, upon reception of the API data, the PIU may cross-check API data of extra-UE flights and selected intra-UE flights against national criminal database and international databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases.

   The API data of the intra-UE flights which have not been selected shall not be subject to the cross check as defined into the previous point.

2. For the purpose of detecting, investigating and prosecuting terrorist offences or serious crimes, the PIU may access data of extra-UE flights and intra-UE flights.

3. Member States may retain data of extra-UE flights and intra-UE flights for a maximum period of three years or according to National legislations after the transfer of such data to the database of the Member State by the router has been completed.

4. Upon expiry of a period of six months after the transfer of the API data related to selected intra-EU flights, API data shall be depersonalised through masking out all data elements which could serve to identify the passenger to whom the API data relate to.

   API data of non-selected intra-EU flights shall be immediately depersonalized after the transfer of such data to the database of the Member State by the router has been completed.

Article 5b

Access of API data by the PIU

1. Where a Member State decides to retain data for the purpose of detecting, investigating and prosecuting terrorist offences and serious crimes, the PIU shall access and respond, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent National authorities or another PIU to provide and process API data in specific cases and to provide the competent authorities or, where appropriate, Europol with the results of such processing.

2. Where the API data has been depersonalized, the disclosure of the full API data shall be permitted only where it is reasonably believed that it is necessary for the purposes referred to in previous point and approved by a judicial authority or another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an ex-post review by that data protection officer.

LITHUANIA

Lithuania welcomes European Commission initiative to regulate the collection and processing of API data for law enforcement purposes and thus complement the legal regulation of PNR. This proposal will allow the handling of passenger data for law enforcement purposes much more efficiently by integrating API and PNR data. Therefore, we express our support for:

- the obligation for carriers to collect API data of all operated flights by automated means - this will significantly increase the quality of data;

- additional data collection at the moment of check-in;

- possibility to collect API data through the router.

Having regard to the opinion of some MS, Lithuania supports the initiative to create flexible opportunities for the PIU to receive all data from the router while the selection and deletion of data from intra-EU flights would be ensured by the PIUs. MS should have the option to choose whether the PIU receives all data or only those selected by the router. We believe that this proposal does not contradict with the decision of the CJEU, as the PNR data of intra-EU flights will have to be selected and deleted by the PIUs.

Therefore, we would also like to support IT proposal to provide for a different data storage regime when processing data for different purposes, i. e. prevention and investigation of serious and terrorist crimes. This approach is based on practical day-to-day experience and objective criteria of processing PNR data. To our knowledge this proposal does not conflict with the provisions of the CJEU decision requiring the establishment of objective criteria for both PNR and API data processing

Seeking to ensure legal clarity, Lithuania proposes to determine in the main part of the text (not in preamble) provision that all API data, collected in accordance with this regulation are processed by PIU ‘s in accordance with the procedures, which are establishes in PNR directive, including the procedure on data depersonalization and data storage.

Article 6

We believe that the provisions of the two proposals for API regulations should be harmonized, providing for flexibility regarding the data controller in the Member States. The "one-stop shop" or “single window” system of passenger data processing applied by Lithuania and some other member states must be taken into account, when the API data controllers are the police or another institution, which later submits the data to the institution responsible for border protection by technical means.

Article 10

The provision of point 20 of the preamble of this Regulation, which provides for the possibility of collecting PNR data through the router, should be established in the text. From this point of view, the European Commission should adopt delegated acts regarding the formats and protocols for transferring PNR data through the router. Therefore, we propose to add these provisions to Article 10, supplementing it with paragraph 3 and 4.

In article 10 add paragraphs 3, 4 and wording it as follows:

3. In accordance with Regulation (EU) 2018/1726, Member States may entrust eu-LISA with the task of facilitating connectivity with air carriers in order to assist Member States in the implementation of Directive (EU) 2016/681, particularly by collecting and transferring PNR data via the router under the same conditions as applied to API data, i.e. without any costs for Member State.

4. The Commission is empowered to adopt delegated acts to supplement this Regulation by laying down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of PNR data to the router.

Article 12

Lithuania, like many Member States, are concerned about this article. We lack clarity as to what exactly the costs of the Member States, related to their connection to the router and integration into it, could be covered by the funds of the European Union. We are in favor of the most flexible conditions for using the Union funds to cover the costs incurred by the Member States related to their connections with the router and integration with it. We propose to establish flexibility regarding the costs covered by the EU budget, as there are MS that have systems developed within their own internal resources though costs are required for internal management resources for such projects.

between the competent law enforcement authorities of the Member States. Moreover, in view of the different nature of the purposes of facilitating border controls and law enforcement, it is appropriate to establish a distinct legal framework for the collection and transfer of API data for each of those purposes.

(3) Directive (EU) 2016/681 of the European Parliament and of the Council[3] lays down rules on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Under that Directive, Member States must adopt the necessary measures to ensure that air carriers transfer PNR data, including any API data collected, to the national Passenger Information Unit ('PIU') established under that Directive to the extent that they have already collected such data in the normal course of their business. Consequently, that Directive does not guarantee the collection and transfer of API data in all cases, as air carriers do not have any business purpose to collect a full set of such data. Ensuring that PIUs receive API data together with PNR data is important, since the joint processing of such data is needed for the competent law enforcement authorities of the Member States to be able to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime. In particular, such joint processing allows for the accurate identification of those passengers that may need to be further examined, in accordance with the applicable law, by those authorities. In addition, that Directive does not specify in detail which information constitutes API data. For those reasons, complementary rules should be established requiring air carriers to collect and subsequently transfer a specifically defined set of API data, which requirements should apply to the extent that the air carriers are bound under that Directive to collect and transfer PNR data on the same flight.

Commented [A1]: 'any API data collected' sees to PNR-data elements (like the other 18 PNR-data elements). All or just some of of these PNR-data elements can be present in a PNR-message (see Appendix 1 of ICAO doc 9944 ('PNR data elements') and Annex 1 of EU Directive 2016/681 ('Passenger name record data as far as collected by air carriers')). Mentioning 'any API data collected' is therefore superfluous and could be deleted.

(4) It is therefore necessary to establish at Union level clear, harmonised and effective rules on the collection and transfer of API data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

(5) Considering the close relationship between both acts, this Regulation should be understood as complementing the rules provided for in Directive (EU) 2016/681. Therefore, API data is to be collected and transferred in accordance with the specific requirements of this Regulation, including as regards the situations and the manner in which that is to be done. However, the rules of that Directive apply in respect of matters not specifically covered by this Regulation, especially the rules on the subsequent processing of the API data received by the PIUs, exchange of information between Member States, conditions of access by the European Union Agency for Law Enforcement Cooperation (Europol), transfers to third countries, retention and depersonalisation, as well as the protection of personal data. Insofar as those rules apply, the rules of that Directive on penalties and the national supervisory authorities apply as well. This Regulation should leave those rules unaffected.

(6) The collection and transfer of API data affects the privacy of individuals and entails the processing of personal data. In order to fully respect fundamental rights, in particular the right of respect for private life and the right to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union ('Charter'), adequate limits and safeguards should be provided for. In particular, any processing of API data and, in particular, API data constituting personal data, should remain limited

[3] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, this Regulation lays down the rules on:

(a) the collection by air carriers of advance passenger information data ('API data') on extra EU flights and ~~selected~~ intra EU flights;

(b) the transfer by air carriers to the router of the API data;

(c) the transmission from the router to the Passenger Information Units ('PIUs') of the API data on extra-EU flights and selected intra-EU flights.

Commented [A2]: This wording seems to imply that air carriers only need to collect API data on selected intra EU flights, while they need to collect data on all flights and the selection is made at the level of the router. We would propose to delete 'selected'.

Article 2

Scope

This Regulation applies to air carriers conducting scheduled or non-scheduled extra-EU flights or intra-EU flights.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(a) 'air carrier' means an air transport undertaking as defined in Article 3, point (1), of Directive (EU) 2016/681;

(b) 'extra-EU flights' means any flight as defined in Article 3, point (2), of Directive (EU) 2016/681;

(c) 'intra-EU flight' means any flight as defined in Article 3, point (3), of Directive (EU) 2016/681;

(d) 'scheduled flight' means a flight as defined in Article 3, point (e), of Regulation (EU) [API border management];

(e) 'non-scheduled flight' means a flight as defined in Article 3, point (f), of Regulation (EU) [API border management];

(f) 'passenger' means any person as defined in Article 3, point (4), of Directive (EU) 2016/681;

(g) 'crew' means any person as defined in Article 3, point (h), of Regulation (EU) [API border management];

(h) 'traveller' means any person as defined in Article 3, point (i), of Regulation (EU) [API border management];

(i) 'advance passenger information data' or 'API data' means the data as defined in Article 3, point (j), of Regulation (EU) [API border management];

1. The router shall, immediately and in an automated manner, transmit the API data, transferred to it by air carriers pursuant to Article 4, to the PIUs of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, or to both in the case of intra-EU-flights. Where a flight has one or more stop-overs at the territory of other Member States than the one from which it departed, the router shall transmit the API data to the PIUs of all the Member States concerned.

   For the purpose of such transmission, eu-LISA shall establish and keep up-to-date a table of correspondence between the different airports of origin and destination and the countries to which they belong

   However, for intra-EU flights, the router shall only transmit the API data to that PIU in respect of the flights included in the list referred to in paragraph 2.

   The router shall transmit the API data in accordance with the detailed rules referred to in paragraph 3, where such rules have been adopted and are applicable.

2. Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. Those Member States shall, in accordance with Article 2 of that Directive, regularly review and where necessary update those lists and shall immediately provide eu-LISA with any such updated lists. The information contained on those lists shall be treated confidentially.

   Commented [A3]: It should be clear that it is still possible to (temporarily) select *all* intra-EU flights, in case a Member State is confronted with a genuine and present or foreseeable terrorist threat.

   Commented [A4]: It is important that eu-LISA will also immediately process the updates to the lists.

3. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

CHAPTER 3

LOGGING, PERSONAL DATA PROTECTION AND SECURITY

Article 6

Keeping of logs

1. Air carriers shall create logs of all processing operations under this Regulation undertaken using the automated means referred to in Article 4(3). Those logs shall cover the date, time, and place of transfer of the API data.

2. The logs referred to in paragraph 1 shall be used only for ensuring the security and integrity of the API data and the lawfulness of the processing, in particular as regards compliance with the requirements set out in this Regulation, including proceedings for penalties for infringements of those requirements in accordance with Articles 15 and 16.

CHAPTER 4

MATTERS RELATING TO THE ROUTER

Article 10

PIUs' connections to the router

1. Member States shall ensure that their PIUs are connected to the router. They shall ensure that their national systems and infrastructure for the reception and further processing of API data transferred pursuant to this Regulation are integrated with the router.

   Member States shall ensure that the connection to that router and integration with it enables their PIUs to receive and further process the API data, as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner.

2. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 11

Air carriers' connections to the router

1. Air carriers shall ensure that they are connected to the router. They shall ensure that their systems and infrastructure for the transfer of API data to the router pursuant to this Regulation are integrated with the router.

   Air carriers shall ensure that the connection to the router and the integration with it enables them to transfer the API data as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner.

2. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 12

Member States' costs

Commented [A5]: As mentioned in the context of the API border management proposal, NL is of the opinion that additional funding for the implementation of the API regulations will be necessary, as the current programmes would not sufficiently cover the costs of implementation.

1. Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union.

   However, the following costs shall be excluded and be borne by the Member States:

   (a) costs for project management, including costs for meetings, missions and offices;

(b) costs for the hosting of national information technology (IT) systems, including costs for space, implementation, electricity and cooling;

(c) costs for the operation of national IT systems, including operators and support contracts;

(d) costs for the design, development, implementation, operation and maintenance of national communication networks.

2. Member States shall also bear the costs arising from the administration, use and maintenance of their connections to and integration with the router.

Article 13

Actions in case of technical impossibility to use the router

1. Where it is technically impossible to use the router to transmit API data because of a failure of the router, eu-LISA shall immediately notify the air carriers and PIUs of that technical impossibility in an automated manner. In that case, eu-LISA shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

2. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 10 of a Member State, the PIU of that Member State shall immediately notify the air carriers, the other PIUs, eu-LISA and the Commission of that technical impossibility in an automated manner. In that case, that Member State shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

3. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 11 of an air carrier, that air carrier shall immediately notify the PIUs, eu-LISA and the Commission of that technical impossibility in an automated manner. In that case, that air carrier shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

Commented [A6]: As mentioned in the context of the API border management proposal, NL would propose to add a paragraph which obliges air carriers to transfer all API data to the router which was not transferred due to the technical impossibility, as soon as it becomes possible to do so. This would mean the second block of text in each of the paragraphs below should be deleted.

After all, the API data could still be useful for asylum claims and for statistics, as well as for the prevention, detection, investigation and prosecution of terrorist offences and serious crime within the context of the API Law enforcement proposal. As such, Member States should receive the API data which was not transferred due to a technical impossibility, as soon as it becomes possible to do so via the router, and as long as it serves the purpose of the API proposals.

Commented [A7]: During the IXIM of 23 January it was explained that when there are issues on the side of the MS, API data would be 'queued' in the router until the moment the transmission to the border authorities or PIUs is completed. In our view it is thus not necessary to inform the air carrier. We would therefore like to suggest to delete the mention of 'the air carriers' in this paragraph.

POLAND

Article 1

"Article 1

Subject matter

For the purposes of the preventing, detecting, investigating and prosecuting of terrorist offenses and serious crime, this Regulation lays down rules on:

a) the collection by air carriers of advanced passenger information data ('API data') on extra EU flights and ~~selected~~ intra-EU flights;"

Retaining the wording of Art. 1 in the form specified in the original version of the draft may lead to a security gap, especially with regard to intra-EU flights, which is mentioned in the explanatory memorandum to the draft in question.

In particular, taking into account the globalization of criminal networks, their constant evolution (flexible and quick changes of routes in response to the actions of law enforcement authorities), diversity, international character and dynamically changing structure of connections, it should be ensured that the router collects data from all flights from and to the EU. It will be up to Member States to select from which flights API data are of interest for the prevention of terrorist offenses and serious crime. Such an approach will provide flexibility with regard to the API data already transferred by the router to the PIU, only for flights included in the list referred to in Article 5. Thanks to this approach, it will be possible to react more quickly to changing modus operandi. Many years of experience show that the process of connecting an air carrier is multi-stage, and sometimes very time consuming.

Article 12

Adjusting the IT infrastructure of the MS to the requirements of the regulation will generate high additional cost as relevant financial resources will be necessary to complete the process. Taking into account that the programming of funds under ISF has been concluded and national programmes already accepted by the Commission the use of these funds to support national efforts will be difficult, if not impossible. Therefore we suggest indicating either a thematic facility of the ISF or EU general budget as the source of financing of all indicated expenses.

Article 16

Article 16 of the draft of the Regulation is very general, and the rules for imposing penalties on air carriers are not specified, but left to the Member States. The content of the provision does not indicate what nature of the penalty may be, in particular, it does not specify whether the penalty may be an administrative instruction or whether it is to be an obligatory financial penalty. There are no ranges of financial penalties specifying their minimum and maximum values. The current wording of the provision does not contain a catalogue of events that exclude the liability of the carrier. The content of the article does not provide the premises excluding the possibility of imposing penalties on the carrier, e.g. due to:

- vis major;

- failure of the system, i.e. the router;

- a failure on the side of the carrier, not attributable to him, provided that eu-Lisa is informed before the deadline for the transfer of data and the subsequent transfer of data.

For this reason, Member States are quite free to define such events in their national law, which can lead to wide divergences in the application of this regulation. Additionally, taking into account the wording of the draft provision, there is no definition of eu-LISA's liability. Can eu-LISA itself request to penalize carriers in the absence of data, incorrect data received from the air carrier? The rule says only on the possibility of imposing penalties by Member States for infringement of the provisions of the Regulation. How to verify who is responsible for the infringement? There is no definition of infringement in the provision, who determines what an infringement is? Is a violation only the failure to provide data, or also the transfer of data after the deadline, the transfer of data in the wrong protocol and format (who verifies the errors? Member State? eu-Lisa?) In this situation, does eu-LISA submit a request to the PIU to punish the carrier?

ROMANIA

Article 5 – Transmission of API data from the router to the PIUs

As regards the obligation to draw up and submit to eu-LISA a selective list of intra-EU flights of interest, we believe that it is necessary to identify a balanced solution taking into account the CJEU ruling in case C-817/19 on the PNR Directive.

We believe that API data as part of the PNR data collected from intra-EU flights represents an important law enforcement tool for tracking the movements of known suspects and identifying the travel patterns of unknown people who may be involved in criminal/terrorist activities.

We understand the importance of having safeguards in place when processing a large amount of personal data and agree with maximising the role of the personal data supervisory authority in conjunction with strengthening the control exercised over how the PIU processes data. But in the same context, it is of utmost importance to maximise all the tools at our disposal to prevent and combat serious crime and terrorism, in order to support the competent authorities in their specific work.

We have taken on board the comments of the other Member States and the feedback from the COM on this issue.

In practice, there are cases where PIU is notified by the competent authority that a person of interest will travel in the next few hours on an intra-EU route. In light of the future regulation that particular route might not have been selected by the PIU. As a result, the PIU will request eu-LISA to receive API data from that route as well from that moment.

In this regard, there are concerns in relation to the agility of the router to swiftly make available API data from that particular route in case of operational need to tackle a risk/vulnerability/threat.

Bearing in mind the operational need and the possible disruptions that might occur, we propose that the on/off switch for selected routes should be performed at the PIU level and not eu-LISA, considering the aforementioned rationale to be in line with the provisions of the court ruling.

FINLAND

In cooperation with other Nordic countries Finland has found one challenge concerning the current API Law Enforcement proposal. It is related to the Nordic passport union which was established already in 1954 by a treaty between the Nordic countries. The Nordic passport union is also recognized for example in the Treaty of the Functioning of the European Union, protocol 19. Under the passport union treaty, Nordic citizens can travel within Nordic countries without passport or other travel document. The Nordic passport union can be seen as a part of Nordic identity and it was respected also during the COVID-19 pandemic when the internal border controls were in force.

We have found that the Article 4 paragraph 3 of the API law enforcement proposal is in contradiction with the Nordic passport union. This article requires the travellers' data to be collected from the travellers' travel documents (even in the case of manual data collection). In practice that would mean that the Nordic citizens would have to have a passport or travel document also when travelling within Nordic countries. For us it is important to respect the traditional Nordic citizens' travel document free movement between Nordic countries and this is a highly important political issue.

Most favorable solution, and taken into account Finland's position in this matter, would be the full exemption concerning the API law enforcement regulation for Nordic citizens who travel between the Nordic countries.

Alternatively, if the full exemption is not possible, we would like to suggest some new wording to amend the Article 4(3). One possibility could be to allow data collection without automated or manual reading of travel documents or other identification documents, where this is necessary due to an international agreement such as the Nordic Passport Union. Such an exemption would also entail an exemption from the obligation for the air carriers to collect data as referred to in API BM article 4 nr. 2 litra c and d. Second possibility could be to allow the data collection from other proof of travellers identity than passport or travel document (where an international agreement between member states and/or Schengen associated countries deems it necessary). In this option a Nordic citizen would not have to own a passport or other travel document, which would respect the passport union up to a certain level. We are open for seeking alternative possibilities as well.