Council of the European Union

Brussels, 17 February 2023
(OR. en)

6230/2/23
REV 2

LIMITE

IXIM 22
ENFOPOL 56
FRONT 48
AVIATION 24
DATAPROTECT 34
JAI 133
COMIX 71
CODEC 154

Interinstitutional File: 2022/0424(COD)

PUBLIC

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	CM 1313/23; 15720/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC - Compilation of replies by delegations

Following the request for written contribution on the above-mentioned proposal (CM 1313/23), delegations will find in Annex a compilation of the replies as received by the General Secretariat.

ANNEX

WRITTEN REPLIES SUBMITTED BY DELEGATIONS

PUBLIC

BELGIUM

Chapter 3:

General remark:

Considering the complexity of this chapter and the plethora of services that we need to consult to provide clear and pertinent remarks, we would like to remind that we expressed a scrutiny reservation that is still relevant.

Article 9:

- Having in mind the general remark on multimodality, as expressed during the IXIM-meetings and the paper delivering the remarks on chapter 1 of the draft API BM Regulation, we'd suggest replacing the words air carrier by carrier;

- The router will consist of a secure channel communication channel for the transmission of the API data. Which measures will be taken to ensure this secure communication channel? Will there be guarantees in place for the information security (the security of the data e.g. protection against hacking) and confidentiality?

- We are interested in the follow-up on the proposals by Hungary and Romania to generate automatic messages to the router regarding the reception of the data. This seems to be a good suggestion.

Article 10:

repetition of the same remark on the term air carrier as stated for article 9.

Article 11:

- Article 11 stipulates that the router shall transmit the data in pursuant to article 6. At the same time, if data need to be corrected after the first push, this will be included in the second data push. This brings us to the question what will happen if there is any inaccurate data still left in this second push, discovered either at carrier side or at government side, will there be a third push then or how would be dealt with in this?

- Regarding the table of correspondence between the different airports of origin and destination and the countries to which they belong, if the extension is made to other modes of transports train stations, ports and applicable bus stations (bus stops) have to be added;

- In §3 – We could appreciate having more information on the necessary rules mentioned for the access of authorized staff members. Information is mentioned on the creation and updating of a list of profiles, but could it be more precise? The Commission mentioned that those details will be provided in a "delegate act" but we would appreciate receiving more insight about what, exactly, could be included in these "details";

- Belgium supports the remarks of Germany and Slovakia regarding the difference in standards and data formats as well as the need to have clarity on this point.

PUBLIC

Article 12:

- Echoing what was said by the Netherlands last time about data storage in the router, we reiterate our question on data retention and statistics. We also question the principle that data should be deleted immediately and permanently. In this case, as explained by the Commission in the last WP, the data will be kept if it is "strictly necessary". However, we still do not understand how it is possible to provide statistics afterward? We recommend making this more explicit in the text.

- Recital 19 mentions that the router will only serve for the transmission of the data and that it will not be a repository of data. Nevertheless, the same recital mentions that any storage of the API data on the router should remain limited to what is strictly necessary for technical purposes related to the transmission. So will there be just logs that are stored or are we envisaging something else here? How will be determined what is strictly necessary?

Article 13:

repetition of the same remark on the term air carrier as stated for article 9.

Article 14:

- Repetition of the same remark on the term air carrier as stated for article 9;

- We're wondering however if there is any back-up solution is envisaged in case the router will be out for a longer period of time for any sort of reason. Will the data that could not be transmitted to the router due to a failure, need to be transmitted once that the router is back in business? Meaning there could be a serious delay in the transfer of the data, or are we switching then to any sort of business continuity plan allowing us to receive the data in another manner temporarily? Is this something for delegated or implementing acts or more for the text of this regulation? We're of the opinion that a certain back-up solution in case of failure of the router is needed, certainly for longer term outages and in that sense support the proposals from The Netherlands and France. If no back-up solution is provided and the data are queued, we support the proposal of the Netherlands to include a paragraph that the carriers need to send the data as soon as possible once the router is back in business;

- Articles 6(1), 4(1) and 8(1) are not applicable in case of failure of the router. Why exclude article 4(1) since a failure of the router does nog prohibit carriers to already collect the API data? Idem for article 8(1), if the carriers could already collect the data.

- Referring back also to the intervention of The Netherlands during the IXIM meeting of 23 January 2023, we're wondering whether or not we should include in this article, in a recital or somewhere else an incentive or even an obligation for EU-LISA and other agencies involved to use to a maximal extent those systems, procedures, practical modalities already in place for other systems such as EES and ETIAS, in order to avoid duplication of work and make use of the budget in a cost-effective manner. This might seem as something logic but just a suggestion to make this more explicit somewhere in the text.

CZECHIA

CZ Comments on Chapter 3 of API regulation (15720)

Article 9

- The Czech Republic welcomes that the router shall share and re-use the technical components of web service and carrier gateways referred to in paragraph 3.

Article 11

- The requirement for Member States to designate the competent border authorities authorised to receive the API data and to establish appropriate rules should also be required from eu-LISA and its staff, given that in certain circumstances eu-LISA staff will have access to data, e.g. in Article 23(3) or Article 31(5).

Article 13

- The General Data Protection Regulation (in particular Articles 24, 30 and 32 thereof) already specifies air carriers' obligations and sets out generally applicable rules. For this reason, the Czech Republic does not consider detailed regulation of logging to be necessary.

Article 14

- The Czech Republic would welcome if the article regulating the procedure and rules in cases where it is not possible to ensure the exchange of API data for technical reasons included alternative solutions for the transmission of API data transmission. The obligation for carriers to provide API data should be maintained even in situations when any technical problem prevents automatic exchange via a central router. There is already a connection between PIU and air carrier and we should consider using this communication channel as an alternative way for the transfer of data in cases when the connection to the router is not available. At the moment, it is unclear whether this solution would find support in the applicable legislation and whether the PIU could play the role of a "postman" in justified and exceptional situations. This could be a practical solution, however, we have doubts regarding data processing purposes (law enforcement X border management).

- In addition, the error notification sent out by the router should indicate the nature of technical problem, since technical problems may occur for a number of reasons. This information could serve as an important factor affecting the initiation of administrative proceedings.

PUBLIC

GERMANY

IXIM, 23th january 2023

DE: written comments on chapter 3

PUBLIC

General comments

DE legal and technical reviews are still ongoing. Against this backdrop, DE mantains the scrutiny reservation on the entire regulatory proposals.

Article 9

Regarding the proposal to introduce a central router, we still have numerous legal and operational questions and see problems that require more in-depth consideration. For the reasons stated in our written statement of January 26th 2023, we are still sceptical of the proposed central router.

Therefore we kindly ask COM to answer the following fundamental legal questions:

1. Why is it considered necessary to process API data centrally by the router, although decentralised transferring directly from the air carriers to the PIU should remain the case for other PNR data and member states are only given the option to use the router for processing PNR data?

2. We ask COM to explain why the transfer to the router of API data on all intra-EU flights is in line with the requirements of the CJEU, although the CJEU in its judgment of 21 June 2022 also requires a restriction to certain intra-EU flights for the transfer and not only for the processing of PNR data, as can be seen in para. 174 of the judgment and in para. 7 of the operative provisions of the judgment (cf. the comments in para. 96 et seqq, according to which the transfer of the data already constitutes a separate encroachment on fundamental rights compared to the storage of the data).

3. Is it from a technical point of view reasonable that in future there will be a coexistence of the processing of API data with the help of a central IT infrastructure at EU level on the one hand and decentralised processing of PNR data on the other?

The fundamental questions about the necessity and proportionality (in terms of fundamental rights and the subsidiarity principle) of the coexistence of a central IT infrastructure for API data with decentralized data processing under the PNR Directive, which were already presented in the first session, continue to arise.

We would also like to point out a few operational aspects:

1. API data cannot be processed per se, since the air carriers do not consider the PAXLIST standard as binding and the standard offers room for interpretation. Bilateral agreements between the recipient of the data and the air carriers are mandatory in this respect.

In operational terms, centralization would require permanent functional and technical harmonization of the respective national and European PNR systems as well as API systems. Would this not require an additional, permanent and transnational committee with the aim of harmonising national IT systems? (How is the data to be understood?) Shouldn't this body be mandated to reach agreements with the airlines (i.e. What codes are permissible and used? Are non-standard-compliant codes still permissible?)?

From the comments of COM in response to the corresponding DE question in the IXIM meeting on 23th Januar 2023, DE understands that COM also considers a standardization of data formats and data transmission to be necessary and feasible. From DE's point of view, the regulation should therefore contain a concrete reference to this purpose, for example in Art. 6 para. 3 API border management.

In addition, it would be essential for the router to have a component that detects any deviations from the mandatory standard (measurement of standard compliance) and automatically provides the airlines with corresponding feedback.

In addition, if data is transmitted via a central routing mechanism, real-time flight information would have to be made available by the router so that any failure to deliver data can be detected automatically.

2. In principle, the question arises as to whether eu-LISA is capable of ensuring the necessary high availability of the system. Any delays in the sphere of eu-LISA lead to restrictions in the performance of (border) police tasks. Therefore, high demands have to be placed on eu-LISA not only during the set-up of the system, but also during its operation. In regard to the multiple tasks eu-LISA is taking on now and in the coming years (including SIS, EES, ETIAS, ECRIS-TCN, interoperability, Prüm II, E-CODEX, JIT platforms), DE has serious doubts that eu-LISA can meet these high demands.

DE thanks COM and eu-LISA for the presentations on the functioning of the router at the meeting. The components mentioned in article 9 paragraph 3 have different purposes and functionalities. We kindly ask for an explanation of why the share and re-use of the technical components is legally mandatory.

Article 10

SWE Chair asked MS at the Jan 23, 2023 meeting to comment on whether they plan to use the router to transmit PNR data as well. There are no DE plans to do so.

PUBLIC

Article 11

DE asks COM to explain:

1. We understood the explanations of COM in the IXIM meeting on 23th January 2023 in such a way that the member states should be free to decide whether the data are transmitted directly from the router to the competent border authority responsible for the airport (and thus several interfaces go out from the router) or whether the member state uses a central distribution point for the forwarding to the competent border authority (and thus only two interfaces go out from the router - one to the distribution point for the border authorities and the second to the PIU). Furthermore, we understood KOM to say that the wording of Article 11 para. 1 does not prevent the establishment of a central distribution point to the border authorities by the member states. Is this correct?

2. Based on the IXIM meetings to date, we assume that API data will be forwarded by the router unchanged. Therefore there is a compelling need for a binding standard specification for the purpose of further processing and for the purpose of sanctioning (see also above on Art. 9) and measurement of standard compliance. Only then a central routing mechanism can be considered from DE perspective.

We would ask COM to consider whether the adoption of delegates acts should not be made mandatory in Article 11 para. 1 by means of appropriate wording. Article 11 para. 4 refers to the "necessary detailed rules".

Should it read "states" instead of "countries" in the second subparagraph of Article 1 para. 1 subpara. 2 or was the term "countries" chosen with regard to the term "country code" (cf. Article 4 para. 2 (e))?

Article 12

With regard to the sanctioning of air carriers according to Articles 29 and 30, COM explained in the meeting on 23th January 2023 that the proof of a violation by an air carrier against an obligation from the regulations should be made possible by means of the logs. It must be ensured that the member states receive the logs for the purpose of sanctioning if required. In DE opinion, it is not yet clear from the regulation how the member state can receive the logs from eu-LISA (e.g. on request?). We consider an explicit regulation to be necessary.

DE reserves comments on Article 12(b) in the discussion of the corresponding provisions of the API law enforcement proposal, in particular on the question whether the transmission of API data of all EU flights to the router is in line with the requirements of the ECJ judgment of 21th June 2022 on the PNR Directive. We refer to our general scrutiny reservation on the two regulations and our written comments in the follow-up to the IXIM meeting on 11/12th January 2023, dated 26th January 2023. We kindly ask COM to explain why the transfer to the router of API data on all intra-EU flights is in line with the requirements of the CJEU, although the CJEU in its judgment of 21 June 2022 also requires a restriction to certain intra-EU flights for the transfer and not only for the processing of PNR data, as can be seen in para. 174 of the judgment and in para. 7 of the operative provisions of the judgment (cf. the comments in para. 96 et seqq, according to which the transfer of the data already constitutes a separate encroachment on fundamental rights compared to the storage of the data).

Article 13

The requirements for airlines in paragraph 2 are less specific than the requirements for eu-LISA in paragraph 1. We request that a provision such as in paragraph 1 letter e be included in the text of the regulation for airlines as well.

According to Article 5, second subparagraph, eu-LISA and the air carriers may keep the logs longer under certain conditions. DE thanks COM for the explanation at the last meeting and the openness to suggestions for wording. From our point of view, replacing "may" with "shall" seems to be a preferable wording.

Article 14

DE asks COM to exlplain the division of tasks between eu-LISA and the "competent national supervisory authority". The direct technical connection is between the airlines and eu-LISA. Shouldn't technical problems in the transmission from the air carrier to eu-LISA also be clarified at this level? From a practical point of view, clarification of the technical connection of the carriers to the router can only be done by eu-LISA.

DE doubts as to whether it is compatible with Art. 4 no. 7 of the GDPR that the national border authorities are classified as solely responsible for data processing under data protection law (Art. 15) and eu-LISA as a mere processor (Art. 16). This is contradicted by the fact that the router is an IT infrastructure operated by eu-LISA, the concrete design of which falls entirely within eu-LISA's area of responsibility and over which the national border authorities have no influence. Is this not a case of joint data responsibility within the meaning of Article 28 of the GDPR or Article 28 of Regulation (EU) 2018/1725? What considerations were decisive for these role assignments?

It is unclear why the obligation to collect data from the carriers is suspended if forwarding via the router is not possible. This precludes a catch-up of the data transmission.

PUBLIC

SPAIN

Written contributions (Articles 9-14) by Spanish IXIM Delegation

As a general remark, since some delegations raised the proposal for the API data to be used for secondary movement controls, this Delegation don't see this as a possibility nor from a practical point of view neither from a legal perspective.

Article 9. The router

No comments.

Article 10. Exclusive use of the router

In this article the use of the router also for PNR data processing the point of view of the Spanish delegation is favourable. The investments for airline connections are costly and difficult, for MS it involves dealing with hundreds of airlines, managing their issues, etc. Therefore, the benefits are clear and the data will arrive anyway.

Article 11. Transmission of API data from the router to the competent border authorities

In the case of changes in destination, how does the MS find out where the arrival was scheduled?. Let us elaborate with an example: the MS has received data about a flight that in the end will not arrive, they do not receive a cancellation, they are expecting passengers that do not arrive and they do not have a notification to delete the data. Only the change is sent to the new destination.

Article 12. Deletion of API data from the router

No comments.

Article 13. Keeping of logs

While the router must store logs (all information related to the flight without including personal data (data that would have to be defined in an Act of Delegation or Execution) the MS must have the ability to store their copy of the logs (they may not match due to incidents).

This data can be used for the sanctioning procedure of sending or not sending, but if the problem is in the data itself, it would not serve as evidence. For example, if all travellers report passport number 1 as their passport number, this is punishable and there would be no traces beyond the 48-day retention period, or if the LEA extends its retention.

It is also unclear in this article whether data received in error, i.e. data that are not within the scope of the regulation, are deleted. It is not clear to us whether this would be included in paragraph 5 of the article on "lawfulness of the processing operations".

PUBLIC

Article 14. Actions in case of technical impossibility to use the router

If there are technical problems with different resolution times, some of them may be long and the flight has already arrived and some of them may not.

In case the flight has not arrived the information will always be useful for borders and in any case it will always be useful for LEA, the connection with the other regulation has to be seen. Recital 24 refers to the fact that they are not useful once the flight has arrived, but the article does not make any difference to this.

In the view of this Delegation, the data can be required as long as the flight has not landed, even further. There may be long flights and the problem with the router may have been solved while flying. In this case the data will be useful if they are available before landing and in any case, in connection with the LEA regulation, they must always be sent.

PUBLIC

FRANCE

NOTE DE COMMENTAIRES DES AUTORITES FRANCAISES

Objet: Note de commentaires suite à l'IXIM du 23 janvier 2023 sur le règlement API 729 « Frontières » (chapitre III, articles 9 à 14)

Réf.: COM (2022) 729 – Règlement API « Frontières »

Suite au groupe IXIM des 11-12 janvier 2023, durant lequel les articles 1 à 8 du règlement 729 ont été abordés (chapitres 1 et 2), la Présidence a organisé une nouvelle réunion du groupe IXIM le 23 janvier, où ont été abordés les articles 9 à 14, soit le chapitre III relatif au routeur.

Par conséquent, les Etats membres sont invités à transmettre leurs commentaires sur les articles consacrés au routeur (chapitre III) suite à cette réunion.

Chapitre III: Dispositions relatives au routeur

En préambule, les autorités françaises aimeraient revenir sur le diaporama présenté en support de l'intervention d'Eu-LISA lors de la réunion IXIM du 23 janvier. Elles expriment les interrogations suivantes:

- **aux diapositives 4, 5 et 6**: la temporalité n'est pas claire. L'agence Eu-Lisa considère que les données iAPI seront obligatoirement transmises à l'enregistrement 48h avant l'embarquement. L'enregistrement en ligne par le passager est actuellement possible en fonction des conditions prévues par chaque compagnie. Est-ce à dire que le règlement API imposera une temporalité harmonisée à 48 heures pour l'enregistrement ouvert au passager avant le départ de son vol?

-à la diapositive 4 – « *Data exchange with airline systems for inbound flights* »:

- les Etats membres reçoivent les iAPI et les lots API (« *batch* »). Comment cela se passe-t-il en pratique? Les iAPI sont-ils transmis au fil de l'eau?

- de plus, une iAPI ne permet pas d'affirmer que la personne est bien dans l'avion. Seul l'API « *batch* » (liste complète effective après fermeture de la porte) le permet. Cela signifie-t-il que chaque Etat membre devra mettre en place un contrôle de cohérence entre les iAPI reçues au fur et à mesure et les lots API (« *batch* ») afin de confirmer ou d'infirmer la présence à bord de la personne?

- Enfin, les lots API ne sont jamais transmis en une seule fois (on parle alors de "part"). Qui s'assure que les données de la totalité du vol attendu ont bien été reçues et comment?

PUBLIC

-concernant les autres diapositives:

- comment se passe la transmission lorsqu'il n'existe pas de système de contrôle des départs (DCS ou *Departure Control System*)? Cela est notamment le cas de l'aviation d'affaire mentionnée dans le règlement ou des compagnies non régulières.

- sur la diapositive relative à l'architecture proposée, eu-Lisa semble imposer le format de transmission PAXLST XML aux Etats membres pour la réception des données. Ce point doit être clarifié car cela nécessitera une évolution obligatoire des systèmes d'informations des Etats membres. Le format XML reçu par les Etats membres n'est pas un format connu et probablement normé au niveau aérien. Est-ce un format nouveau créé par eu-Lisa en dehors de toute norme internationale? Cela impliquerait un coût financier significatif pour chaque Etat membre ainsi qu'une durée de développement très importante.

De plus, à nouveau en guise de remarques générales, les autorités françaises s'interrogent sur deux aspects tirés de la future mise en œuvre du présent règlement API:

- la mise en place du routeur aura-t-elle un impact sur le rôle des fournisseurs de données qui transmettent actuellement les données API entre la compagnie aérienne et l'Unité d'Information Passager - UIP (guichet unique en France)? Ainsi, pour la collecte des données iAPI interactives, nous avons bien compris que celles-ci seront transmises par le simple fait de consulter la passerelle des transporteurs prévue par le règlement EES, sans intervention nécessaire des fournisseurs de données. Mais pour la collecte des lots de données API (« *batch* ») à la fin de l'embarquement, par quel biais les compagnies aériennes transmettent-elles ces données et est-ce à dire que les fournisseurs de données continueront à jouer un rôle à cette étape précise pour transmettre les données vers le routeur?

- concernant les données API collectées au titre de la mise en œuvre de la directive PNR 2016/681 (cf. rubrique 18 de l'annexe I): les données API seront-elles forcément collectées par le routeur et quel est le règlement API qui servira de base juridique dans ce cas (règlement API « contrôle frontières » ou règlement API « répressif »)?

Enfin, les autorités françaises notent que le règlement « prévention/répression » est parfois cité au sein de cette proposition de règlement « frontières », comme à l'article 12 par exemple où le point *b* lui est dédié. Il est souhaitable que le texte apporte des clarifications sur l'articulation entre les deux propositions de règlement, de manière à ce que ces références soient mieux comprises.

Article 9: Le routeur

Concernant le paragraphe 2: si la connexion au routeur via internet apparaît privilégiée, quel sera le protocole de messagerie utilisé en alternative pour la transmission des données?

Si on suit la logique de la Commission dans sa rédaction de l'article 1 points b) et c), il manque au point 2 (b) de l'article 9 la transmission des données API depuis le routeur vers les autorités compétentes. Seul le transfert (depuis les transporteurs vers le routeur) y est mentionné. Les autorités françaises souhaitent que cela soit explicité dans le texte.

Comme le précise le paragraphe 3, l'intérêt du routeur est de profiter de la mise en œuvre du système EES en partageant et réutilisant les briques techniques de ce système pour collecter les données API, notamment la passerelle des transporteurs. La plus-value de cette mutualisation a été avancée par la Commission comme un argument de facilitation pour les transporteurs aériens.

La France a mis en avant à plusieurs reprises son souhait de la multi-modalité du routeur. Or il faut prendre en compte deux types de difficultés concernant justement la mise en œuvre d'EES auxquelles l'agence doit faire face à ce jour:

- **les problèmes relatifs à la conduite du projet EES,** liés, notamment, à un manque de ressources pour piloter ses contractants.

- **les problèmes liés à l'enregistrement des transporteurs.** L'agence indique rencontrer un succès mitigé dans sa campagne auprès des transporteurs pour qu'ils interconnectent leurs applicatifs d'embarquement au futur « web service EES ». A ce jour, seuls 934 transporteurs et deux fournisseurs de services ont débuté leurs tests.

Les difficultés rencontrées par l'agence eu-Lisa pour le système EES risquent de se retrouver avec le routeur API. **Il est donc essentiel que cette dernière soit dotée des ressources humaines nécessaires** afin de tenir les délais imposés par le législateur et de mener une véritable politique d'influence auprès des transporteurs. Les écosystèmes des transporteurs aériens, maritimes, ferroviaires et routiers étant totalement différents, les moyens affectés à cette dernière tâche devront être accrus en proportion du nombre de vecteurs couverts.

Par ailleurs, le portail transporteur EES/VIS/ETIAS ne reçoit des données de la part des transporteurs qu'à une seule reprise (« au plus tôt dans les 48 heures avant l'heure de départ »), uniquement et ne concerne que les ressortissants de pays tiers (en court séjour dans un premier temps jusqu'à l'entrée en service de la refonte VIS, puis ceux aussi en long séjour).

En termes de données transmises, les champs de données envoyées (selon les règlements EES/VIS/ETIAS actuels) au portail transporteur EES/VIS/ETIAS ne correspondent pas entièrement à ceux du projet de règlement API. Quelle est l'harmonisation (technique, juridique) envisagée? Les transporteurs devront-ils envoyer les données API via un canal spécifique et séparé au portail transporteur EES/VIS/ETIAS?

Enfin, au paragraphe 3: il y a une erreur sur la référence d'article, le portail transporteur est mentionné à l'article 45c du règlement 767/2008 (VIS).

<u>Article 10: Utilisation exclusive du routeur</u>

Il y a une incohérence avec l'article 1 concernant les destinataires des données API: il est fait mention des UIP, qui sont déjà au sein de la quasi-totalité des Etats membres, le guichet unique de réception de ces données. Il convient alors d'ajouter le terme "*PIUs*" partout où est mentionné "*competent border authorities*".

En effet, cette nécessaire mention dans le premier article permet de reconnaître la logique du guichet unique des UIP pour la totalité du texte.

La proposition de la Commission ne vise qu'une seule catégorie de transporteurs (« *air carriers* »). La rédaction devra être adaptée à la multi-modalité telle que souhaitée par les autorités françaises.

Article 11: Transmission des données API du routeur aux autorités frontalières compétentes

Le titre de l'article 11 se limite à la transmission des données API du routeur vers les autorités des garde-frontières compétentes. Or, pour être complet et cohérent avec le texte dans son ensemble, il conviendrait de viser également les UIP des Etats membres (sous réserve d'adaptation de l'article 1e, maintien en attendant la nouvelle version de la Présidence).

Article 12: Suppression des données API du routeur

Cet article mentionne un stockage des données API réalisé par le routeur: « *API data, transferred to the routeur […] shall be stored on the router only insofar as necessary to complete the transmission to the relevant competent border authorities or PIUs[…]* ».?

Les autorités françaises appellent l'attention sur le risque de saturation du routeur qui pourrait advenir en raison de la volumétrie très importante des données API, en cas de difficulté dans le transfert vers les autorités compétentes.

La première phrase indique" *to the relevant competent borders authorities or PIU*": l'emploi du OU (*or*) est incohérent avec l'article 10 qui indique ET (*and*) (sous réserve d'adaptation de l'article 1e, maintien en attendant la nouvelle version de la Présidence).

Au point (a), comment pouvons-nous être certains que la transmission des données est complète? Il convient de s'assurer que la totalité des messages transmis couvrent la totalité des passagers et membres d'équipages à bord, et que le vol a bien eu lieu. Nous proposons donc la rédaction complémentaire suivante:

« *where the transmission of the API data to the relevant competent border authorities or PIUs, as applicable, has been completed* ***and justified by their reception confirmation ».***

Article 13: Tenue de journaux

Au paragraphe 3, s'agissant de la phrase: " *including proceedings for penalties for infringements of those requirements in accordance with Articles 29 and 30 of this Regulation*", les autorités françaises soulignent la nécessité pour les Etats membres de disposer également des journaux adéquats pour faire face à de potentiels désaccords, notamment en ce qui concerne les possibles sanctions.

Article 14: Actions en cas d'impossibilité technique d'utiliser le routeur

Les autorités françaises ont pris bonne note des explications apportées par la Commission sur la rédaction de cet article, à savoir qu'en cas de défaillance technique du site de Strasbourg celui de Sankt Johann im Pongau serait en mesure de prendre instantanément le relais sans aucune interruption des transmissions. Il serait intéressant 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 (par exemple, retour au processus actuel avec la transmission des données des transporteurs directement aux UIP?)

PUBLIC

Cet article prévoit les actions en cas d'impossibilité technique d'utilisation du routeur. Cependant, 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. En effet, aucune procédure de secours concrète n'est explicitée en cas d'impossibilité technique d'utiliser le routeur. Il est simplement indiqué que, en cas de panne, eu-LISA est en charge de la réparation du routeur.

Ce point pourrait être développé à l'article 5 (point 2) qui détaille les différents modes de collecte par les transporteurs. Que deviennent les données? Sont-elles conservées par les compagnies? Pour quelle durée? Quels sont les autres moyens de transmission?

L'article 4 point 1 prévoit que les transporteurs aériens collectent les données API dans le but de les transmettre au routeur. Il est logique que cette obligation de transfert des données au routeur ne s'applique pas lorsque ce dernier est en panne. Cependant, il conviendrait de vérifier si en cas de panne du routeur, les transporteurs aériens peuvent toujours collecter les données API, et comment et combien de temps ils devront les conserver. Cette conservation est-elle effectuée chez le transporteur ou dans l'interface qui est utilisée pour que les données soient ensuite envoyées vers le routeur? Une absence de collecte des données API en cas de panne du routeur poserait des difficultés aux autorités compétentes, qui ne disposeront dès lors plus de données essentielles.

A cet égard, l'article 8 de la directive PNR prévoit que, dans l'hypothèse où les transporteurs aériens ont recueilli des données API, mais ne les conservent pas par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, ils doivent également transférer ces données par la méthode « push » à l'UIP de l'État membre visé (dans le cas d'un tel transfert, toutes les dispositions de la directive PNR s'appliquent à ces données API). Il pourrait donc être prévu une transmission des données API vers les UIP (voire également vers les autorités de contrôle aux frontières), *a minima* en cas de panne du routeur, afin d'assurer la continuité de la transmission des données API.

De plus, une suspension limitée dans le temps de l'obligation de transmission des données API, due à une impossibilité technique d'utiliser le routeur, représente un risque.

Aux paragraphes 1, 2 et 3, il convient d'ajouter une référence aux UIP après "*the competent border authorities*".

Au paragraphe 3, les autorités françaises s'interrogent sur les raisons amenant les compagnies aériennes à notifier auprès de la Commission et l'agence Eu-LISA les mesures prises pour résoudre les soucis techniques.

Par ailleurs, il semble que cette notification relève plutôt de la responsabilité des UIP, et non des autorités en charge du contrôle aux frontières. Ne pourrait-on pas modifier le texte en ce sens? Par ailleurs, par quel canal les autorités en charge du contrôle frontières devraient-elle transmettre cette information?

Concernant les incidents, la notification automatique devra-t-elle intervenir pour la survenance des incidents de toute sorte, ou faut-il inclure une notion de durée (incident qui perdure)? Cela devrait être également précisé dans le texte.

Courtesy translation

Following the IXIM meeting of 11-12 January 2023, during which Articles 1 to 8 of the API Regulation 729 were discussed (chapters 1 and 2), the Presidency organised a new meeting on 23 January, where Articles 9 to 14, i.e. Chapter III on the router, were discussed.

Therefore, Member States are invited to send their comments on the articles dedicated to the router (chapter III) following this meeting.

Chapter III: Provisions relating to the router

As a preamble, the French authorities would like to come back on the slides presented in support of Eu-LISA's intervention during the IXIM meeting on January 23. They have the following questions:

- **on slides 4, 5 and 6**: the time frame is not clear. Eu-LISA considers that iAPI data will be transmitted at check-in 48 hours before boarding. Online check-in by the passenger is currently possible depending on the conditions provided by each airline. Does this mean that the API regulation will impose a harmonized timeframe of 48 hours for check-in open to the passenger before the flight's departure?

- **on slide 4** - "*Data exchange with airline systems for inbound flights*":

- Member States receive iAPIs and API batches. How does this work in practice? Are the iAPIs transmitted as they come in?

- Moreover, an iAPI does not confirm that the person is on the plane. Only the "batch" API (complete list effective after closing the door) allows this. Does this mean that each Member State will have to set up a consistency check between the iAPIs received and the API batches in order to confirm or deny the presence of the person on board?

- Finally, API batches are never transmitted in one go (this is called a "share"). Who ensures that the data for the entire expected flight has been received and how?

- concerning the other slides:

- How does the transmission occur when there is no DCS (Departure Control System)? This is particularly the case for the business aviation mentioned in the regulation or for non-scheduled airlines.

- On the slide concerning the proposed architecture, eu-Lisa seems to impose the PAXLST XML transmission format on the Member States for receiving data. This point needs to be clarified as it will require a mandatory evolution of the Member States' information systems. The XML format received by the Member States is not a known and probably standardized format at the aviation level. Is it a new format created by eu-Lisa outside any international standard? This would imply a significant financial cost for each Member State as well as a very long development time.

PUBLIC

In addition, again by way of general remarks, the French authorities have questions about two aspects of the future implementation of the present API Regulation:

- Will the implementation of the router have an impact on the role of the data providers who currently transmit API data between the airline and the Passenger Information Unit - PIU (one-stop shop in France)? For example, for the collection of interactive iAPI data, we understand that it will be transmitted by simply consulting the carrier gateway provided for in the EES regulation, without the need for intervention by data providers. But for the collection of the API data batches at the end of the boarding process, how do the airlines transmit this data and does this mean that the data providers will continue to play a role at this specific stage to transmit the data to the router?

- Regarding API data collected under the implementation of PNR Directive 2016/681 (see item 18 of Annex I): will API data necessarily be collected by the router and which API regulation will serve as the legal basis in this case ("border control" API regulation or "law enforcement" API regulation)?

Finally, the French authorities note that the "law enforcement" regulation is sometimes quoted in this proposal, such as in Article 12, where point b is dedicated to it. It would be desirable to clarify the relation between the two proposals for regulations, so that these references can be better understood.

Article 9: The router

Concerning paragraph 2: if the connection to the router via the Internet appears to be preferred, what will be the alternative messaging protocol used for data transmission?

If we follow the logic of the Commission in its drafting of Article 1 (b) and (c), point 2 (b) of Article 9 lacks the transmission of API data from the router to the competent authorities. Only the transfer (from the carriers to the router) is mentioned. The French authorities would like this to be clarified in the text.

As stated in paragraph 3, the router's interest is to take advantage of the implementation of the EES system by sharing and reusing the technical components of this system to collect API data, in particular the carriers' gateway. The added value of this mutualisation has been put forward by the Commission as a facilitation argument for air carriers.

France has repeatedly emphasized its desire for a multi-modal router. However, two types of difficulties must be taken into account concerning the implementation of EES, which the agency is currently facing:

- **problems related to the conduct of the EES project**, linked in particular to a lack of resources to pilot its contractors;

- **problems with carrier registration**. The agency reports mixed success in its campaign to get carriers to connect their boarding applications to the future EES web service. To date, only 934 carriers and two service providers have begun testing.

The difficulties encountered by the eu-Lisa agency with the EES system are likely to be repeated with the API router. **It is therefore essential that the agency be provided with the necessary human resources** to meet the deadlines imposed by the legislator and to conduct a real policy of influence with the carriers. Since the ecosystems of air, maritime, rail and road carriers are totally different, the resources allocated to this task will have to be increased in proportion to the number of vectors covered.

Furthermore, the EES/VIS/ETIAS carrier portal receives data from carriers only once ("*at the earliest 48 hours before departure time*"), and only for third-country nationals (initially for short stays until the VIS recast comes into operation, and then for long stays).

In terms of transmitted data, the data fields sent (according to the current EES/VIS/ETIAS regulations) to the EES/VIS/ETIAS carrier portal do not fully correspond to those of the draft API regulation. What harmonization (technical, legal) is envisaged? Will carriers have to send API data via a specific and separate channel to the EES/VIS/ETIAS carrier portal?

Finally, in paragraph 3: there is an error on the article reference, the carrier portal is mentioned in article 45c of regulation 767/2008 (VIS).

Article 10: Exclusive use of the router

There is an inconsistency with Article 1 concerning the recipients of API data: it mentions PIUs, which are already in almost all Member States the one-stop shop for receiving these data. The term "*PIUs*" should therefore be added wherever "*competent border authorities*" are mentioned.

In fact, it is necessary to mention it in the first article to recognize the logic of the “one-stop shop” of the PIUs for the entire text.

The Commission's proposal refers to only one category of carriers ("*air carriers*"). The wording will have to be adapted to multi-modality as desired by the French authorities.

Article 11: Transmission of API Data from the router to Competent Border Authorities

The title of Article 11 is limited to the transmission of API data from the router to the competent border authorities. However, in order to be complete and consistent with the text as a whole, it should also refer to the PIUs of the Member States (subject to adaptation of Article 1, to be maintained pending the new Presidency version).

Article 12: Deletion of router API data

This article mentions the storage of API data by the router: "*API data, transferred to the router [...] shall be stored on the router only insofar as necessary to complete the transmission to the relevant border authorities or PIUs* [...]".

The French authorities draw attention to the risk of saturation/overload of the router that could occur due to the very large volume of API data, in case of difficulties in the transfer to the competent authorities.

The first sentence states "*to the relevant competent borders authorities or PIU"*: the use of *"or"* is inconsistent with Article 10, which states "*and*" (subject to adaptation of Article 1, to be maintained pending the new version of the Presidency).

In (a), how can we be sure that the transmission of data is complete? It must be ensured that all the messages transmitted cover all the passengers and crew members on board and that the flight actually took place. We therefore propose the following additional wording:

"*where the transmission of the API data to the relevant competent border authorities or PIUs, as applicable, has been completed* ***and justified by their reception confirmation***".

Article 13: Keeping of logs

In paragraph 3, with regard to the phrase: "*including proceedings for penalties for infringements of those requirements in accordance with Articles 29 and 30 of this Regulation*", the French authorities stress the need for Member States to have adequate logs to deal with potential disagreements, particularly with regard to possible penalties.

Article 14: Actions in case of technical impossibility to use the router

The French authorities have taken good note of the explanations provided by the Commission on the wording of this article, namely that in the event of technical failure of the Strasbourg site, the Sankt Johann im Pongau site would be able to take over instantly without any interruption of transmissions. It would be interesting to have more details on the existence of a back-up system and its operation. An alternative procedure in case of technical failure of the router should be proposed to limit any risk of failure (e.g. return to the current process with transmission of data from the carriers directly to the PIUs?)

This article provides for actions in case of technical impossibility of using the router. However, nothing is provided for as an alternative in the event of a router malfunction, apart from notification of the authorities and carriers by the eu-LISA Agency. In fact, no specific backup procedure is explained in the event that it is technically impossible to use the router. It is simply stated that, in the event of a breakdown, eu-LISA is responsible for repairing the router.

This point could be developed in Article 5 (point 2), which details the different methods of collection by the carriers. What happens to the data? Are they kept by the companies? For how long? What are the other means of transmission?

Article 4(1) requires air carriers to collect API data for the purpose of transferring it to the router. It is logical that this obligation to transfer the data to the router does not apply when the router is down. However, it should be verified whether in the event of a router failure, air carriers can still collect the API data, and how and for how long they will have to retain it. Is this retention done at the carrier or at the interface that is used for the data to be sent to the router? Failure to collect API data in the event of a router failure would create difficulties for the competent authorities, who would then no longer have essential data.

PUBLIC

In this regard, Article 8 of the PNR Directive provides that, in the event that air carriers have collected API data, but do not retain it by the same technical means as other PNR data, they must also transfer this data by the "push" method to the PIU of the Member State concerned (in the event of such a transfer, all the provisions of the PNR Directive apply to this API data). Provision could therefore be made for the transmission of API data to the PIUs (or even to the border control authorities), at least in the event of a router failure, in order to ensure the continuity of API data transmission.

Furthermore, a time-limited suspension of the obligation to transmit API data due to a technical impossibility to use the router represents a risk.

In paragraphs 1, 2 and 3, a reference to the PIUs should be added after "*the competent border authorities*".

In paragraph 3, the French authorities wonder why the airlines are notifying the Commission and the EU-LISA agency of the measures taken to resolve the technical problems.

Moreover, it seems that this notification is the responsibility of the PIUs and not of the authorities in charge of border control. Couldn't the text be modified in this sense? Furthermore, through which channel should the authorities in charge of border control transmit this information?

With regard to incidents, should automatic notification take place for incidents of any kind, or should a notion of duration be included (incident that continues)? This should also be specified in the text.

PUBLIC

LITHUANIA

General position regarding the router

Lithuania strongly supports centralized data collection through the router and believes that such data collection will reduce the administrative burden for both PIU's and air carriers, ensuring that all Member States (MS) will receive data of equal volume and quality. However, it is necessary to evaluate certain threats related to possible router failures, i.e. according to the provisions of the Proposal, air carriers are exempted from the obligation to transfer API data electronically in case of the router failure. There is no clarity if the data available at the time of the failure, the air carriers must transfer it by other means of communication directly to the PIU's or later electronically to the router. This vulnerability could lead to loss of API data in case of a failure.

Proposals to add provisions to the articles:

Regarding Article 10

In order to ensure the possibility for member states to submit a request to eu-Lisa for the collection of PNR data via the router in accordance with Regulation (EU) [API law enforcement], it is necessary to supplement this Regulation (EU) with such provision in the text, not in the preamble. There should be established possibility to use the router for the transmission of the PNR data on a voluntary basis and free of charge.

In article 10 add paragraph 2, as follows:

The router can also be used to transmit PNR data, on the same conditions as API data, if member states apply to eu-Lisa.

Regarding Article 14

This article specifies what measures the authorities must take if, due to technical failures, it is not possible to transfer data to the router. However, there is no clarity if the data must be transferred by the air carriers by other means of communication directly to the PIU's later. This vulnerability could lead to loss of API data in case of a failure. We suggest to clarify Article 14 of this Regulation (EU) establishing an obligation for air carriers to transfer data as soon as the router becomes operational.

HUNGARY

Comments from the Hungarian delegation

PUBLIC

Subject: Chapter 3 (Articles 9-14) of the Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC

We still do not yet have an overall national position; the national coordination process is still ongoing with the involvement of all the national stakeholders.

With this in mind, however, we would like to reiterate our support for the objectives of the draft Regulation and its Chapter 3.

Regarding Article 11:

During the API data transmission from the router, the appropriate technical safeguards and mechanisms need to be implemented to deal with technical obstacles and errors regarding incorrect, incomplete data transmissions. When designing the API router, implementing the appropriate safeguards and clearly defining the responsibilities regarding data quality are essential.

The possibility of resending data needs to be clarified in cases where they are not received, delayed, or incorrectly delivered.

It should be also discussed if a function could be implemented, which sends feedback to the API router when data has been correctly received and processed by the competent authorities.

Regarding Article 14:

Furthermore, alternative solutions in case of technical impossibility to use the router must be developed in the draft Regulation, particularly when technical obstacles persist for extended periods.

PUBLIC

CHAPTER 3

PROVISIONS RELATING TO THE ROUTER

Article 9

The router

1. eu-LISA shall design, develop, host and technically manage, in accordance with Articles 22 and 23, a router for the purpose of facilitating the transfer of API data by the air carriers to the competent border authorities and to the PIUs in accordance with this Regulation and Regulation (EU) [API law enforcement], respectively.

2. The router shall be composed of:

   (a) a central infrastructure, including a set of technical components enabling the transmission of API data;

   (b) a secure communication channel between the central infrastructure and the competent border authorities and the PIUs, and a secure communication channel between the central infrastructure and the air carriers, for the transfer of API data and for any communications relating thereto.

3. Without prejudice to Article 10 of this Regulation, the router shall, to the extent technically possible, share and re-use the technical components, including hardware and software components, of the web service referred to in Article 13 of Regulation (EU) 2017/2226 of the European Parliament and of the Council[1], the carrier gateway referred to in Article 6(2), point (k), of Regulation (EU) 2018/1240, and the carrier gateway referred to in Article 2a, point (h), of Regulation (EC) 767/2008 of the European Parliament and of the Council[2].

---

1 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

2 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

Article 10

Exclusive use of the router

The router shall only be used by air carriers to transfer API data and by competent border authorities and PIUs to receive API data, in accordance with this Regulation and Regulation (EU) [API law enforcement], respectively.

Article 11

Transmission of API data from the router to the competent border authorities

1. The router shall, immediately and in an automated manner, transmit the API data, transferred to it pursuant to Article 6, to the competent border authorities of the Member State referred to in Article 4(3), point (c). It shall do so in accordance with the detailed rules referred to in paragraph 4 of this Article, where such rules have been adopted and are applicable.

   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.

2. The Member State shall designate the competent border authorities authorised to receive the API data transferred to them from the router in accordance with this Regulation. They shall notify, by the date of application of this Regulation referred to in Article 39, second subparagraph, eu-LISA and the Commission of the name and contact details of the competent border authorities and shall, where necessary, update the notified information.

   The Commission shall, on the basis of those notifications and updates, compile and make publicly available a list of the notified competent border authorities, including their contact details.

3. The Member States shall ensure that only the duly authorised staff of the competent border authorities have access to the API data transmitted to them through the router. They shall lay down the necessary rules to that effect. Those rules shall include rules on the creation and regular update of a list of those staff and their profiles.

4. The Commission is empowered to adopt delegated acts in accordance with Article 37 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.

PUBLIC

Article 12

Deletion of API data from the router

API data, transferred to the router pursuant to this Regulation and Regulation (EU) [API law enforcement], shall be stored on the router only insofar as necessary to complete the transmission to the relevant competent borders authorities or PIUs, as applicable, in accordance with those Regulations and shall be deleted from the router, immediately, permanently and in an automated manner, in both of the following situations:

(a) where the transmission of the API data to the relevant competent border authorities or PIUs, as applicable, has been completed;

(b) in respect of Regulation (EU) [API law enforcement], where the API data relates to other intra-EU flights than those included the lists referred to in Article 5(2) of that Regulation.

Article 13

Keeping of logs

1. eu-LISA shall keep logs of all processing operations relating to the transfer of API data through the router under this Regulation and Regulation (EU) [API law enforcement]. Those logs shall cover the following:

   (a) the air carrier that transferred the API data to the router;

   (b) the competent border authorities and PIUs to which the API data was transmitted through the router;

   (c) the date and time of the transfers referred to in points (a) and (b), and place of transfer;

   (d) any access by staff of eu-LISA necessary for the maintenance of the router, as refererred to in Article 23(3);

   (e) any other information relating to those processing operations necessary to monitor the security and integrity of the API data and the lawfulness of those processing operations.

   Those logs shall not include any personal data, other than the information necessary to identify the relevant member of the staff of eu-LISA, referred to in point (d) of the first subparagraph.

2. Air carriers shall create logs of all processing operations under this Regulation undertaken by using the automated means referred to in Article 5(2). Those logs shall cover the date, time and place of transfer of the API data.

PUBLIC

3. The logs referred to in paragraphs 1 and 2 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 and Regulation (EU) [API Law Enforcement], including proceedings for penalties for infringements of those requirements in accordance with Articles 29 and 30 of this Regulation.

4. eu-LISA and the air carriers shall take appropriate measures to protect the logs that they created pursuant to paragraphs 1 and 2, respectively, against unauthorised access and other security risks.

5. eu-LISAand the air carriers shall keep the logs that they created pursuant to paragraphs 1 and 2, respectively, for a time period of one year from the moment of the creation of those logs. They shall immediately and permanently delete those logs upon the expiry of that time period.

However, if those logs are needed for procedures for monitoring or ensuring the security and integrity of the API data or the lawfulness of the processing operations, as referred to in paragraph 2, and these procedures have already begun at the moment of the expiry of the time period referred to in the first subparagraph, eu-LISA and the air carriers may keep those logs for as long as necessary for those procedures. In that case, they shall immediately delete those logs when they are no longer necessary for those procedures.

Article 14

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 competent border authorities 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 6(1) 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) and Article 8(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 20 of a Member State, the competent border authorities of that Member State shall immediately notify the air carriers, the competent authorities of the other Member States, 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 6(1) 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) and Article 8(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 21 of an air carrier, that air carrier shall immediately notify the competent border authorities, 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 6(1) 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) and Article 8(1) shall not apply either to the API data in question during that time period.

When the technical impossibility has been successfully addressed, the air carrier concerned shall, without delay, submit to the competent national supervisory authority referred to in Article 29 a 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.

POLAND

Dear Presidency, Dear Colleagues,

please find below PL comments to the chapter III of API proposal:

PL maintains an analytical reservation and can only provide preliminary comments at this time. PL's position may change after full, formal arrangements have been made.

Detailed Comments on the draft on the Chapter 3 of the Proposal for a Regulation:

Matters related to the processing of API data and the creation of a central router, which will be prepared by eu-LISA, generally do not raise any objections to PL. However, there is an additional question to be resolved in the context of the transfer of API data to PIU, i.e. the entity processing PNR data, which also includes API data. According to the definition contained in the draft regulation, a passenger is both a “passenger” and “a crew member”. In the context of the implementation of the information flow via the router, will it be possible to transfer data only on “passengers” without data on “crew members”? Will the data, however, be transferred to the PIU automatically, without selecting the data concerning the crew? This is important from the point of view of the analysis of PNR data and the possibility of further action by PIU.

PUBLIC

ROMANIA

As a general remark, RO appreciates that a key factor in the development of the system in order to serve its specific purposes is to collect high quality data. We took note of the arguments presented by eu-LISA and COM during the meetings of IXIM WP and we are convinced that this component will be greatly improved through this new legislative package and that the discussions within the future API Committee will converge to a solution to prevent situations caused by certain errors in the transmission of API data.

Chapter III:

Article 10 – Exclusive use of the router

We took note of the arguments presented by COM on the use the router for the transmission of PNR data. At this stage, making use of the possibility is under national analysis.

Preliminary, we consider that the inclusion of a legally binding provision in the API proposals should be further explored and the opinion of the Council Legal Service on the possibility to amend PNR Directive through API Regulations is much appreciated. Furthermore, the question arises as to whether the article 16 para. 4 from eu-LISA mandate could be invoked as a sole legal ground for the transmission of PNR data using the router legally setup for API data, according to art. 10.

Another point that still needs to be clarified from a legally point of view is the transmission of API data in a decentralised manner as part of PNR data set, in accordance with PNR Directive.

Another important aspect that should be reflected on is the additional costs to be borne by the MSs in order to use the router for the transmission of PNR data, and the financial support that could be provided to MSs through the Internal Security Fund.

Article 12 – Deletion of API data from the router

Concerning letter b), please note that RO has a scrutiny reservation linked to the future discussions on API LEA proposal.

Article 14 – Actions în case of technical impossibility to use the router

As a general remark, we propose to include in the text the possibility for air carriers to use alternative means to transmit API data, namely the channels already established and which respects the requirements of legality, security and efficiency, for receiving API data at the level of MSs. This solution will lead to ensuring business continuity of API data transmission. Our text proposal is the following: **New para. 4. Where it is technically impossible to use the router to transmit API data due to the situations described at paragraphs 1, 2 and 3, the air carriers shall transmit to competent border authorities, through alternative means, the API data in question.**

Also, RO considers that the notifying procedure included in para. (3) should also be mirrored in art. 6 para. (4), so that the air carrier informs eu-LISA and the border authority simultaneously about the inaccurate, incomplete and no longer up – to- date data.

PUBLIC

SLOVENIA

Slovenia supports proposals that define clear rules for the collection and transfer of API data. We believe that the proposed regulation improves operational cooperation and reduces related costs, while at the same time facilitating border control and, most importantly, unifying conditions and rules.

However, we believe that the Regulation should be expanded and, in addition to the obligation to collect API data for air transport, also collect passenger data when passengers board ships and railways. In doing so, we are aware of the problems of carriers, especially in rail transport, which would have a major impact on this segment of the industry. With the introduction of the ETIAS Regulation, the issuance of customized tickets and identity verification upon boarding in rail and bus transport will become standard practice and will not require high additional investments when collecting API or PNR data. In the future, we expect an increased use of rail transport, and it would be appropriate to consider extending the API Regulation to rail transport as well.

Slovenia supports the creation of a central router and the proposed technical solution, which should make the most of the available components and the already established infrastructure developed within the framework of interoperability. We are also of opinion, that the proposed central router should also include the exchange of PNR data. We would like to ask for the opinion of the Commission here:

- Is the use of a central router to transfer PNR data compatible with the PNR Directive?
- Is it possible to combine the PNR Directive and the API Regulation?
- The member states incurred costs with the establishment of the PIU units, and the national system will need to be adapted to the new system envisaged by the new Regulation. Is EU funding planned for this?

We also support the possibility of accepting API and PNR data via the central router according to the "Single Window" principle, and after acceptance at the national level, the relevant unit decides where to forward the data. In this regard, it would be necessary to further examine the possibility of enabling PIU units to transfer the appropriate set of data to the competent border authorities. We believe that it is currently unclear whether this solution would find support in the current legislation and whether PIU could play the role of "national router" in justified and exceptional situations. This could be a practical solution.

SLOVAKIA

Article 9, point 1

1. We would like to ask to add to Article 9, point 1, that the router can be used for facilitating the transfer of PNR data as well as of API data. The aim for the suggestion is to not limit the functionality of the router only for API data.

Article 10

2. In Article 10, we would like to add "and other means of transportation" after the "air carrier" as we consider the original formulation too limiting, considering the possibility of collecting API data from other means of transportation in the future.

Article 11, point 1, paragraph 1

3. In Article 11, we would respectfully ask to add "PIU" along with "border authorities of the Member State". The reason for that is that in the cases of a "single window" setup, the PIUs are the first recipients of API data that they then transmit to competent border authorities through a shared system and as a result should be included in the Directive as well.

Article 11, point 1, paragraph 2

4. Still concerning Article 11, we would also like to pose a question if it would be possible for eu-LISA to share the table of correspondence mentioned in the second paragraph of point 1 with Member state competent authorities. This table of correspondence would be necessary for border authorities and PIUs to retain overview about which air carriers are connected and operating flights within their country as well as keeping in mind the connectivity with ETIAS.

Article 12

5. For Article 12, we would like to pose a question if it would be possible to keep the API data in router for at least 48 hours before deletion. The purpose is to be able to react to instances, where due to a sudden change in circumstances, a previously no-risk flight becomes extremely important for collection of data for purposes of Law Enforcement and in respect to Regulation (EU) [API law enforcement]. One example would be the perpetrator of terrorist attack using previously no-risk flight either to enter the country before the attack or to try to flee the country after the attack. In this instance, we would not be able to collect any API data to use for Investigation and Law Enforcement, as they would be immediately deleted.

Article 13

6. For Article 13, we would like to pose a question if it would be possible for Member state authorities to have access to the router logs eu-LISA keeps and if yes, under what conditions? Access to the logs will be necessary for purposes of administrative actions in cases of non-compliance of air carriers with Directive.

PUBLIC

Article 14, points 1, 2 and 3

7. In Article 14, points 1, 2 and 3 we would like to suggest adding “PIU” after “competent authorities”, technical impossibility to use the router will affect the law enforcement activities of PIUs as well and thus informing them about such situations can be vital. Additionally we would also like to ask what is meant by the term “automated means” in the text of Article 14. Will it be in form of automated e-mail message, or through some other means.

Article 14

8. Additionally for Article 14, we would like to suggest changing it so that Articles 4, 6, 8 will still apply during the period of technical impossibility to use the router and give air carriers an obligation to store the data for a certain period and transfer them once the technical issues are resolved. While the data from the period of technical impossibility to use router are no longer relevant for border control, they can be still vital for PIUs and for the purpose of law enforcement.

PUBLIC

FINLAND

Article 11 paragraph 1

"The router shall, ~~immediately and in an automated manner~~ **after performing checks to relevant databases, automatically** transmit the API data, transferred to it pursuant to Article 6, to the competent border authorities of the Member State referred to in Article 4(3), point (c). It shall do so in accordance with the detailed rules referred to in paragraph 4 of this Article, where such rules have been adopted and are applicable.

Article 13 does not take into account the possible support of the Frontex permanent force to the member states. We could propose an amendment to paragraph 3 as follows:

"The Member States shall ensure that only the duly authorised staff of the competent border authorities **or designated members of the standing corps of the European Border and Coast Guard agency** have access to the API data transmitted to them through the router. They shall lay down the necessary rules to that effect. Those rules shall include rules on the creation and regular update of a list of those staff and their profiles.

Article 14 does not recognize compensatory actions if, for example, the router is broken. We could introduce a new paragraph 4, for example:

"In the situations defined in the first, second and third paragraph of this Article, competent border authorities of the Member states may ask air carriers to provide API data, concerning selected flights based on risk analysis, directly to them by other technical means."

PUBLIC

SWITZERLAND

Switzerland thanks you for the opportunity to submit its written comments. Please find below our comments on Articles 11 and 13 of the proposal for a Regulation on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC.

Article 11, Transmission of API data from the router to the competent border authorities

Paragraph 1: During the discussions of 23 January on Article 11, the Commission stated that the router forwards the data to the competent national border control authority at the destination airport. What is the situation in this respect for a multi-leg flight that takes off in a third country and then flies to different Member States, where the passengers on the same flight cross the external border in different countries? Is the router able to forward the passenger data to the correct authorities based on the departure and destination airports?

We would welcome if the router not only forwarded the data transmitted by the airlines, but also checked them for completeness (does the number of passengers and crew members match the number of passenger records transmitted?) and plausibility (unrealistic or impossible birth dates, etc.) and gave appropriate feedback to the airline transmitting the data so that it could correct missing or implausible data by means of a push, thus ensuring that the competent border control authorities had reliable data in time to be able to perform their tasks.

Article 13, Keeping of logs

The result of the aforementioned completeness and plausibility checks should also be stored in the log data.

PUBLIC