EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

8 February 2023

Opinion 6/2023

on the Proposals for Regulations on the collection and transfer of advance passenger information (API)

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under ***Article 42(1)*** *of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the 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 (COM/2022/729 final), and the 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 (COM/2022/731 final).

This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the two Proposals that are relevant from a data protection perspective.

Executive Summary

On 13 December 2022 the European Commission issued two legislative proposals on the collection and transfer of advance passenger information ("API"): a Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for enhancing and facilitating external border controls ("API Border management Proposal"), and a 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 ("API Law enforcement Proposal") (together "the Proposals").

The objective of the API Border management Proposal is enhancing and facilitating the effectiveness and efficiency of border checks at external borders and combating illegal immigration, and replacing the existing Council Directive 2004/82/EC ("API Directive"). The objective of the API Law enforcement Proposal is to lay down better rules for the collection and transfer of API data by air carriers for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime, complementing the existing Directive (EU) 2016/681 ("PNR Directive").

Taking into account that the data processing operations that would result from the Proposals correspond to or complement already existing data processing operations provided for in Union law, the Opinion focuses primarily on the necessity and proportionality of the envisaged processing of API data from intra-EU flights and its compatibility with the PNR Directive as interpreted by the CJEU judgment in case C-817/19.

While the EDPS considers the proposed solution for intra-EU flights broadly sufficient to ensure compliance with the CJEU judgment on Article 2 of the PNR Directive, he nevertheless invites the co-legislators to consider the development of harmonised criteria for the selection of intra-EU flights, from which API data should be collected, in line with the conditions spelled out by the Court. Furthermore, the EDPS recommends further strengthening of the security of processing of API data in the router with additional safeguards, such as pseudonymisation and/or encryption of the API data, if technically and operationally feasible.

The Opinion also provides other specific recommendations, such as the need to explicitly clarify in the Proposals that in case of technical impossibility of the router to transmit the API data transferred by the air carriers to the competent national authorities, the data should be automatically deleted.

Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ('EUDPR')[1], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 13 December 2022 the European Commission issued two legislative proposals on the collection and transfer of advance passenger information ("the Proposals"):

- a 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 ("API Border management Proposal"),

- a 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 ("API Law enforcement Proposal").

2. The objective of the API Border management Proposal is enhancing and facilitating the effectiveness and efficiency of border checks at external borders and combating illegal immigration[2], thus replacing the existing Council Directive 2004/82/EC ("API Directive"')[3].

3. The objective of the API Law enforcement Proposal is to lay down better rules for the collection and transfer of API data by air carriers for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime[4], complementing the existing Directive (EU) 2016/681 ("PNR Directive")[5].

4. The Proposals are consistent with the Schengen Strategy of June 2021, presented in the Commission Communication "A strategy towards a fully functioning and resilient Schengen area" which specifically underlined the need for an increased use of API data in combination with PNR data to significantly enhance internal security, in compliance with the fundamental right to the protection of personal data and the fundamental right to

[1] OJ L 295, 21.11.2018, p. 39.
[2] See Article 1 of Proposal API Border management.
[3] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24.
[4] COM(2022) 731 final, Explanatory memorandum to the Proposal API Law enforcement, page 3.
[5] 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. 132–149.

freedom of movement[6]. Moreover, at international level, the United Nations' Security Council and the Organization for Security and Co-operation in Europe (OSCE) also repeatedly called for the establishment and global rollout of API and PNR systems for law enforcement purposes[7].

5. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 14 December 2022 pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 44 of the API Border management Proposal and Recital 29 of the API Law enforcement Proposal. In this regard, the EDPS also positively notes that he has already been informally consulted on the Proposals pursuant to recital 60 of EUDPR.

6. In view of the close alignment between the Proposals[8], including the numerous cross-referencing between them, it seems most appropriate for the EDPS to assess them in a single Opinion.

2. General remarks

7. The EDPS notes that the specific data processing operations provided for in the Proposals correspond to or complement already existing data processing operations, provided for in the Union law. Regarding the API Border management Proposal, it is the legal framework on border checks at the external borders, in particular the Schengen Borders Code[9], and for API Law enforcement Proposal, it is the already mentioned PNR Directive.

8. Furthermore, the EDPS takes into account that the Court of Justice of the European Union (CJEU) in recent case C-817/19[10] confirmed the validity of the PNR Directive, while providing important clarifications on a number of its provisions, including in substance additional limitations on the processing of personal data to ensure compliance with Articles 7 and 8 of the Charter. In particular, the Court laid down a number of conditions that national laws transposing the PNR Directive must comply with relation to the application of the PNR Directive to intra-EU flights.

9. The requirements laid down by the Court in its judgment constitute an important point of reference for the assessment of the Proposals, in particular with regard to the processing of API data from intra-EU flights. In this context, EDPS positively notes the explicit reference to the Court judgment in Recital 14 and in the Explanatory memorandum of the API Law enforcement Proposal [11].

[6] COM(2021) 277 final
[7] UN Security Council Resolutions 2178(2014), 2309(2016), 2396(2017), 2482(2019), and OSCE Ministerial Council Decision 6/16 of 9 December 2016 on Enhancing the use of Advance Passenger Information.
[8] See Recital 11 of Proposal API Law enforcement.
[9] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1–52.
[10] CJEU judgment of 21 June 2022, case C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491.
[11] COM(2022) 731 final, Explanatory memorandum of the Proposal API Law enforcement, page 3.

10. At the same time, it should be borne in mind that the CJEU judgment concerns the processing of PNR data that comprises 18 data categories[12]. API data is only one subset of them. The impact of the processing of API data on the fundamental rights of the passengers could therefore arguably be considered lesser compared to the processing of PNR data, despite the newly created obligation at EU level to collect API data. Furthermore, it should be recalled that air carriers already collect API data during check-in of the passenger (online check-in and at the airport), while at the same time their practices are diverse and inconsistent[13].

11. Finally, as regards the relationship between the two Proposals and the EU legal framework on data protection, the EDPS positively notes the clarification that the generally applicable acts of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 (GDPR)[14], the EUDPR and Directive (EU) 2016/680 (LED)[15], would not be affected by the envisaged API Regulations[16]. However, the EDPS does not deem it useful, nor accurate to indicate that the proposed legislation would 'complement' the generally applicable acts on the protection of personal data, as the proposed act would simply be in line with them, as all sectorial legislation.

3. Processing of API data from intra-EU flights

12. Similarly to the current legal framework - the API Directive and the PNR Directive - the two Proposals make a distinction between extra-EU and intra-EU flights[17]. The API data from extra-EU flights is processed for the purposes of (1) border checks at external borders and of combating illegal immigration (further limited only to flights into the EU), and (2) preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Conversely, the API data from intra-EU flights can be processed only for preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as defined in the PNR Directive, and not for immigration purposes.

13. The EDPS notes that pursuant to Article 2 and Article 4 (1) and (6) of the API Law enforcement Proposal, air carriers would be obliged to collect and subsequently transfer to a "router" the API data on [all] "scheduled or non-scheduled extra-EU flights or intra-EU flights"[18]. The router would then transmit to the Passenger Information Units ('PIU') of the Member States on the territory of which the flight will depart and will land only the API data of the intra-EU flights selected by the Member States pursuant to Article 2 of the PNR

[12] See Annex I to the PNR Directive.
[13] COM(2022) 731 final, Explanatory memorandum of the Proposal API Law enforcement, page 1.
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119, 4.5.2016, p. 1).
[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.
[16] See Recital 25 of API Border management and Recital 17 of API Law enforcement.
[17] See Article 3(c) of API Border management and Article 3(b) of API Law enforcement.
[18] There seems to be a contradiction (possible clerical error) in Article 1(a) of Proposal API Law enforcement, which refers to selected intra-EU flights. However, from Article 4 and the overall explanations in the recitals and the explanatory memorandum (page 10) of the same Proposal, it is clear that the intended selection is to take place after the transfer to the router to avoid disclosing the selected flights.

Directive, as interpreted in the CJEU judgment. To this end, eu-LISA would maintain a confidential list of the selected intra-EU flights, which would be regularly updated[19].

14. The EDPS further notes that according to Article 12(b) of the for API Border management Proposal, the API data from intra-EU flights other than those included in the list would be deleted from the router "immediately, permanently and in an automated manner". Likewise, air carriers would be obliged to immediately and permanently delete the API data from intra-EU flights after the transfer to the router is completed[20].

15. According to the Commission, the proposed technical solution aims to limit the transmission of API data to PIUs to designated flights only and without disclosing confidential information on which intra-EU flights have been selected, in view of the risk of circumvention by the persons involved in serious crime or terrorist activities[21].

16. The EDPS is of the view that when assessing compliance of the proposed solution for intra-EU flights, the conditions set out in the CJEU judgment mentioned above, while being an important point of reference, need to be applied by analogy (*mutatis mutandis*). The Court has clarified that an interference with Articles 7 and 8 of the Charter may be justified by assessing the seriousness of the interference and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness[22]. In the present context, it should be taken into account that the ruling concerns a different system involving, among others, processing of many more categories of personal data than API. As a consequence, the EDPS considers that the Proposal would entail a lower level of interference with those fundamental rights than that considered by the Court.

17. According to the CJEU, EU law, in particular Article 2 of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, precludes national legislation, which establishes a system for the transfer, by air carriers, and for the processing, by the competent authorities, of the PNR data of all intra-EU flights. By contrast, such processing can be allowed when a Member State is "confronted with a terrorist threat which is shown to be genuine and present or foreseeable"[23].

18. In this context, the relevant question is whether the proposed technical solution leads in practice to indiscriminate transfer of API data from all intra-EU flights to the competent national authorities (PIUs), outside the exceptional situations of terrorist threat, or not.

19. In the view of the EDPS, the envisaged automatic processing in the router - the 'filtering' of the API data based on an official list of selected airports or routes, the transmission of data only from pre-selected flights, and the immediate deletion of the data from non-selected flights, precludes the possibility for PIUs to receive and process in any manner API data from intra-EU flights they are not entitled to.

---

[19] See Article 5 and Recital 14 of Proposal API Law enforcement.
[20] Article 4(8)(b) of Proposal API Law enforcement.
[21] COM(2022) 731 final, Explanatory memorandum of Proposal API Law enforcement, page 11.
[22] See CJEU judgments of 21 June 2022, case C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491, paragraph 116, and of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraph 55, and the cited case-law.
[23] CJEU judgment of 21 June 2022, case C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491, p. 7 of the ruling and paragraphs 171 and 173.

20. Moreover, the EDPS considers that collection and transfer to the router of API data, on the one hand, and processing of the API data by the competent national authorities, on the other hand, are intrinsically linked and therefore should not be considered in isolation. Therefore, as it is not only legally precluded but also technically impossible for the Member States to access API data from intra-EU flights they have not formally selected and communicated, then the EDPS considers this element of the Proposals as compliant with the relevant EU law as interpreted by the CJEU.

21. Furthermore, it is the EDPS' understanding that, at this stage, no satisfactory (readily available, technically viable and economically effective) alternative solution exists that would offer comparable guarantees and safeguards for intra-EU flights.

22. For instance, transferring of API data by air carriers for all intra-EU flights directly to the PIUs and leaving it to the Member States to decide which API data is necessary and to delete the rest, appears problematic. It would indeed entail systematic processing by national authorities of data from all intra-EU flights, including those not selected by them.

23. In turn, "filtering" of API data at air carrier level does not offer sufficient guarantees and could create additional challenges related to confidentiality (e.g. circumvention by persons involved in serious crime or terrorist activities), reliability and consistency of the processing, as the API data will be filtered by multiple actors based on instructions from all Member States. In this regard, it should be noted that according to the Impact Assessment to the Proposals, there are currently around 1000 air carriers operating in the EU, and approximately 150 of them operate exclusively within the Union[24].

24. It follows that the processing of all API data taking place at the level of the router in the light of the level of interference with the fundamental rights concerned, the safeguards provided, in particular the legal and technical impossibility for the Member States' PIUs to receive and otherwise process API data not related to the selected flights, remains proportionate to the objective pursued.

25. Finally, the EDPS recalls that in accordance with the CJEU judgment, the selection of intra-EU flights must be limited to what is strictly necessary. To this end, the Member States' choice has to be justified on the basis of [objective] indications and to be subject to regular reviews[25]. Therefore, in order to avoid divergent practices, the EDPS invites the co-legislators to consider introducing provisions, including specific empowerment to the Commission in accordance with Articles 290 and/or 291 TFEU if deemed appropriate, for the development of harmonised criteria and methodology for the selection of intra-EU flights, from which API data should be collected.

4. Security of API data

26. Given the scale of the processing and the affected number of data subjects, the envisaged collection and transfer of API data may create potential risks and therefore must be accompanied by effective safeguards ensuring a high level of security. In this regard, the

[24] SWD(2022) 422 final, Impact Assessment Report, Annex 4, page 71.
[25] See CJEU judgment of 21 June 2022, case C-817/19, Ligue des droits humains, paragraph 174.

EDPS notes that the API Border management Proposal provides for a detailed provision on the security of the API data and the router, in addition to the general obligations on the security of personal data pursuant to Article 33 of the EUDPR and Article 32 of the GDPR[26]. At the same time, the respective provision in the API Law enforcement Proposal[27] is very general and neither provides for any specific measures, nor refers to the relevant rules in the API Border management Proposal.

27. Furthermore, the EDPS recalls the obligation of Member States authorities, air carriers and eu-LISA, to implement appropriate technical and organisational measures in line with the requirements of data protection by design and by default pursuant to Article 27 of the EUDPR, Article 25 of the GDPR and Article 20 of the LED.

28. The EDPS therefore recommends that the API Law enforcement Proposal should provide for specific measures ensuring the security of API data processed for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, or, alternatively, should refer to the relevant rules in the API Border management Proposal.

29. Furthermore, the EDPS recommends to eu-LISA, when designing and developing the router, to consider the use of pseudonymisation and/or encryption of the API data, if technically and operationally feasible.

5. Roles and responsibilities

30. The Proposals would designate the air carriers as controllers, within the meaning of Article 4(7) GDPR, for the processing of API data constituting personal data in relation to their collection of that data and their transfer thereof to the router[28].

31. Furthermore, competent border authorities are designated as controllers in relation to the processing of API data constituting personal data through the router, including the transmission, as well as in relation to their processing of API data constituting personal data under the API Border management Proposal. Similarly, PIUs would 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 through the router, including transmission, under the API Law enforcement Proposal.

32. Finally, eu-LISA is designated as processor within the meaning of Article 3, point (12) of Regulation (EU) 2018/1725 for the processing of API data constituting personal data through the router[29].

33. Given the division of responsibilities between the various actors, interpreted in the light of the relevant provisions of the GDPR, the EUDPR and the LED, and also taking into account the EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725[30] as well as the EDPB Guidelines 07/2020 on the concepts of

[26] Article 17 of Proposal API Border management.
[27] Article 8 of Proposal API Law enforcement.
[28] See Article 15 of API Border management and Article 7 of API Law enforcement.
[29] Article 16 of API Border management.
[30] https://edps.europa.eu/sites/default/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

controller and processor in the GDPR[31], the EDPS considers this designation of roles appropriate, for the following reasons.

34. The EDPS notes that Member States authorities, acting as controllers, determine the purposes and essential means of the processing via the router, within the legal framework established by the Proposals. According to the EDPB Guidelines, "essential means" are closely linked to the purpose and the scope of the processing. Concerning the purposes, although eu-LISA will process all API data, the data eventually processed by the Member States authorities is only the data related to the flights selected by the Member States. The latter therefore determine what specific subsets of data they will receive and "why" within the meaning of the above mentioned EDPB guidelines 7/2020[32]. Concerning the essential means, they are determined by the law: the API data that is presented to eu-LISA; the duration of the processing; the categories of recipients (the competent PIUs and border authorities) and the categories of data subjects whose personal data will be processed (air travellers that fall within the scope of the API Regulations).

35. The "non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hardware or software or the detailed security measures - what eu-LISA is supposed to do - and could be left to the processor to decide on. Moreover, according to the EDPB, it is not necessary that the controller actually has access to the data that is being processed (i.e. to the data in the router).

36. In practice, the eu-LISA is offering a communication channel between the air carriers and the Member State controllers – rather than a standalone database (there is no 'true' storage of API data in the router). The Agency does not have any other purposes for the processing of API data, other than transmitting it to competent controllers in the Member States.

37. Notwithstanding the designation of eu-LISA as processor on behalf of Member States authorities, the Proposals place a significant responsibility for ensuring a lawful and secure processing of the API data in the router on the Agency. eu-LISA has to guarantee, *inter alia*, that only properly selected API data regarding intra-EU flights would reach the PIUs, the deletion of the remaining API data, as well as high level of security to prevent any unauthorised access to the data[33].

38. In this regard, the EDPS recalls that the EUDPR does not make a distinction between controllers and processors with regard to the supervisory powers of the EDPS under Article 58 or the possible sanctions for infringements under Article 66 thereof. In any event, the EDPS plans to closely supervise the exercise of the tasks of eu-LISA under the Proposals, in line with his mandate pursuant to the EUDPR.

6. Reporting and statistics

39. The EDPS notes that, in accordance with Article 31 of the API Border management Proposal, eu-LISA would have the task to store daily statistics from the processing of data in the router in the central repository for reporting and statistics (CRRS) established in

[31] https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
[32] *See* EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, paragraph 35.
[33] See Articles 17, 22-24 of API Border management.

Article 39 of Regulation (EU) 2019/817 (Interoperability Regulation)[34] as well as to produce various statistical reports. To this end, eu-LISA would have the right to access certain API data transmitted through to the router, "without however such access allowing for the identification of the travellers concerned".

40. In his Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability[35], the EDPS has already cautioned that the proposed establishment of CRRS would impose a heavy responsibility on eu-LISA. This position has been repeated in the EDPS Opinions on EES[36], ETIAS[37], SIS[38], VIS[39] and eu-LISA[40]. In this context, the EDPS has made a number of recommendations regarding the CRRS, including on the need for a thorough information security risk assessment, adequate security measures, and privacy by design. These recommendations remain fully valid in the context of the Proposals.

7. Deletion of API data from the router

41. Article 12 of the API Border management Proposal would provide for two situations that would trigger automatic deletion of API data from the router:
(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 API law enforcement Proposal, where the API data relates to other intra-EU flights than those included the lists referred to in Article 5(2) of that Regulation (i.e. not selected by any Member State).

42. The EDPS also notes that Article 14 of the API Border management Proposal describes the actions that have to be taken in case of technical impossibility to use the router. In general, is such situations air carriers would have no obligation to transfer API data to the router. However, the Proposals do not stipulate explicitly what should happen if an air carrier has transferred API data to the router before becoming aware of a technically impossibility of the router to subsequently transmit the API data because of a failure of the systems or infrastructure of Member State(s).

43. The EDPS therefore recommends clarifying in Article 12 of the API Border management Proposal that in case of technically impossibility of the router to subsequently transmit the API data to the competent national authorities, the data is automatically deleted.

[34] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).
[35] https://edps.europa.eu/sites/default/files/publication/2018-04-16_interoperability_opinion_en.pdf
[36] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf
[37] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf
[38] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf
[39] https://edps.europa.eu/sites/default/files/publication/18-12-13_opinion_vis_en.pdf
[40] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf

8. Other comments

44. The EDPS notes that Article 4(1), second sentence of the API law enforcement Proposal specifically clarifies the allocation of the obligation to transfer API data in cases where the flight is code-shared between several air carriers. However, the API Border management Proposal does not include a similar rule. Therefore, the EDPS recommends adding a similar provision on code-shared flights also in the API Border management Proposal.

9. Conclusions

45. In light of the above, the EDPS recommends to the co-legislators to:

(1) consider the development of harmonised criteria and methodology for the selection of intra-EU flights, from which API data should be collected;

(2) provide for specific measures in API Law enforcement Proposal ensuring the security of API data processed for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, or, alternatively, refer to the relevant rules on security in the API Border management Proposal;

(3) clarify in Article 12 of the API Border management Proposal that in cases of technical impossibility of the router to subsequently transmit the API data to the competent national authorities, the data should be automatically deleted;

(4) to clarify in the API Border management Proposal the allocation of the obligation to transfer API data in cases where the flight is code-shared between several air carriers.

Brussels, 8 February 2023

(e-signed)
Wojciech Rafał WIEWIÓROWSKI