European Data Protection Board

Statement

Statement 2/2025 on the implementation

of the PNR Directive in light of CJEU Judgment C-817/19

Adopted on 13 March 2025

Table of contents

The European Data Protection Board has adopted the following statement:

1 BACKGROUND AND PURPOSE OF THIS STATEMENT

1. On 21 June 2022, the Court of Justice of the European Union (CJEU) rendered its Judgment (hereinafter the PNR Judgment) on the 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 (hereinafter the PNR Directive).

2. While the CJEU found that the validity of the PNR Directive was not affected, it ruled that, in order to ensure compliance with the Charter of Fundamental Rights of the European Union (hereinafter the Charter), the PNR Directive needs to be interpreted as including important limitations to the processing of personal data. This, the CJEU held, is of particular importance with a view to the serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter. To limit these interferences to what is strictly necessary, the CJEU identifies several aspects that national laws transposing the PNR Directive must comply with. Among the most relevant are in particular:

    - limitation to the purposes set out in the PNR Directive, which are exhaustive,
    - application of the PNR system only to terrorist offences and serious crime (i.e. ordinary crime is explicitly excluded) having an objective link, even if only an indirect one, with the carriage of passengers by air,
    - limitation of the application of the PNR Directive with regard to intra-EU flights and other means of transport,
    - no indiscriminate application of the general retention period of five years to all air passengers' personal data.

3. In light of the PNR Judgment, on 13 December 2022 the EDPB adopted Statement 5/2022 on the implications of the PNR Judgment for the implementation of the PNR Directive on the use of PNR in Member States[1]. It concluded that the interpretation of the most critical aspects pointed out by the PNR Judgment are of main importance in order to proceed in a harmonized manner in all the Member States. Following up on Statement 5/2022, the EDPB prepared the present Statement with the purpose to provide further guidance on some of the necessary adaptions and limitations to the processing of PNR data for the respective Passenger Information Units (hereinafter PIU) in the Member States that derive from the PNR Judgment. Moreover, the Statement also outlines the necessity for the legislative bodies in the Member States to implement the changes into the national laws and to amend these laws in light of the PNR Judgment as soon as possible. Furthermore, the Statement should also facilitate the application of the PNR Directive and the interpretation thereof in light of the PNR Judgment for legal practitioners as well as Data Protection Officers.

[1] https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-implications-cjeu-judgment-c-81719-use-pnr-member_en .

2 RECOMMENDATIONS

4. The EDPB wishes to make the following recommendations on some of the key aspects of the PNR Judgment for the implementation of the PNR Directive. Each of the recommendations is followed by explanatory remarks following a more detailed assessment and interpretation of the PNR Judgment. Further guidance may be provided if necessary.

2.1 Categories of persons

5. **The personal data of third parties only falls within the scope of the PNR Directive insofar as it relates directly to the flight operated and the passenger concerned. In practical terms, such third party personal data is limited to: (a) the payment information and billing address of a person that purchased the ticket on behalf of the passenger insofar as it directly relates to the flight, and (b) the contact details of a parent or guardian who is dropping off or picking up a passenger who is an unaccompanied minor. All other third-party personal data must be deleted immediately and permanently by the PIU upon receipt.**

6. Annex I of the PNR Directive contains 19 headings which describe separate categories of PNR data which the air carrier must transfer to the PIU. Each category relates to information that passengers either provide themselves as part of the booking process or which are provided on their behalf. Some of these categories are quite broad and could include personal data of other persons besides the passenger (e.g. third parties involved in booking and/or purchasing the flight ticket). The extent to which these additional categories of data subjects involved may be processed needs to be interpreted in light of the Judgment.

7. The information to be provided by the air carrier to the PIU under each heading of Annex 1 of the PNR Directive must be interpreted narrowly in terms of its relationship to the passenger and must be limited to what is strictly necessary to meet the objectives of the PNR Directive, whilst excluding sensitive data[2]. Hence, personal data of data subjects other than the passenger only falls within the scope of the PNR Directive insofar as it relates directly to the flight operated and the passenger concerned, even where this goes against a plain reading of the actual headings.[3] E.g. in the case of Heading 5, only the contact information and address of the passenger is within the scope, even if a third party made a booking on behalf of the passenger[4]. Where a third party has paid for the flight, then their payment and billing information will need to be provided under Heading 6. However, this must be limited to information relating to the payment methods for, and billing of, the air ticket. Other information from third parties must be deleted, as they are not directly related to the flight, except for (a) the payment information and billing address of a third party that purchased the ticket on behalf of the passenger insofar as it directly relates to the flight, and (b) the contact details of a parent or guardian dropping off or picking up a passenger who is an unaccompanied minor.

8. The onus is on Member State PIUs to ensure that any PNR data provided by air carriers in excess of what is permitted under Annex I, read in light of the PNR Judgment, are deleted "immediately and permanently on receipt" to prevent data processing in relation to excessive categories of data subjects.

[2] Judgment of 21 June 2022, C-817/19, EU:C:2022:491. para. 128.
[3] cf. ibid, para 129-131.
[4] Ibid., para. 131.

2.2 Objective link

9. **Offences having no objective link, not even an indirect one, with the carriage of passengers by air cannot justify the application of the system established by the PNR Directive.[5] In order to establish an objective link, there need to be objective criteria to set up a connection between PNR data and combating serious crime and terrorist offences. While a direct link relates to "offences targeting the carriage of passengers by air as well as offences committed during or through travel by air"[6], an indirect link covers all situations where there is no direct link but where serious crime and terrorist offences may be prevented, detected, investigated or prosecuted with the help of processing PNR data of selected connections or flights, i.e., in particular, when air transport is used as a means of preparing such offences or evading criminal prosecution.**

10. Article 1(2) of the PNR Directive provides that PNR data collected in accordance with that directive may be subject to the processing operations referred to in Article 6(2)(a) to (c) only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. According to the CJEU it is for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime[7]. The CJEU establishes that an essential element to assess the necessity and proportionality of the processing activities with regard to PNR data is the existence of an objective link, even if only an indirect one, with the carriage of passengers by air.[8] The recommendation aims to provide further clarification on the nature and relevance of the aspect of "objective link".

11. In order to establish an objective link, there need to be objective criteria to set up a connection between PNR data retained and combating serious crime and terrorist offences.[9] Hence, a supposed connection needs to be supported by facts and evidence; e.g. the purely subjective expectation of a police officer would not be sufficient. Furthermore, each application of the PNR system must be examined in order to evaluate the existence of an objective link. In order to reduce the seriousness of the interference with the fundamental right to protection of personal data, the analysis as to the existence of an objective link needs to take place as early as possible in the process, i.e. in particular before carrying out prior assessments, Article 6(2)(a), and upon requests for subsequent assessment, Article 6(2)(b).

12. When persons are identified by the automated processing, the PIU must refrain from transferring the results to the competent authorities, when, after the review, they do not have anything "*capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime"*[10]. These criteria need to be applied mutatis mutandis also before initiating the assessments of passengers prior to their scheduled arrival in or departure from the Member State, Article 6(2)(a). Already the facts and evidence, on the basis of which travellers are targeted, need to be capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime. The requirement to check the existence of the objective link also upon the individual review following by non-automated means according to Article 6(5) is to be considered as an additional necessary safeguard. Furthermore, already at this stage it is essential to

[5] Ibid., para. 156.
[6] Ibid., para. 155f.
[7] Ibid., para. 152.
[8] Ibid., para. 156f, also cf. para. 191.
[9] Ibid, para. 125 and 251.
[10] Ibid., para. 204.

ensure that the application of the PNR system does not extend to offences that amount to ordinary crime, including by taking into account other features than the maximum penalty.[11]

13. As regards subsequent assessments upon requests by competent authorities, Article 6(2)(b), it is important to note that the CJEU made a distinction depending on whether the PNR data is sought in connection with terrorist offences or in connection with serious crime having an objective link with air travel. Simply put, where the PNR data is sought in connection with serious crime, there must be a demonstrably more rigorous level of assessment of requests by the PIU to meet the "duly reasoned" threshold under 6(2)(b). In order for such requests to be duly reasoned, the PIU must be satisfied that they are based on "*objective material capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air*"[12]. This more rigorous assessment should be set out in the PIU's internal policies and procedures so as to be objectively verifiable, in particular by the supervisory authority. Any request for subsequent disclosure, though – i.e. also requests related to terrorist offences – need to be based on evidence that is likely to substantiate the substantive condition for "reasonable" grounds.[13]

2.3 Intra-EU flights

14. **It is only permissible to apply the PNR Directive to intra-EU flights if the Member States find, following an assessment, that there is a threat of terrorist offences and serious crime, which is capable of justifying the application of the said directive to intra-EU flights.[14] The principle of strict necessity applies notwithstanding the application to selected or all intra-EU flights[15], thus requiring an assessment as regards the time and scope of the application, including for genuine and present or foreseeable terrorist threats. It would not be considered an indiscriminate application if individual assessments have been made for all respective flights, even if in fact all intra-EU flights are covered. Regular and ad-hoc review procedures should be incorporated into the system.**

15. According to Article 2 of the PNR Directive, the Member States may apply the Directive to intra-EU flights.[16] The CJEU in its PNR Judgment made certain restrictions regarding this application of the PNR Directive.[17] A Member State that wishes to apply the PNR Directive to either all intra-EU flights under Article 2(2) or only for selected flights under Article 2(3) needs to ensure throughout the assessment,

[11] Cf. ibid., para. 151f.
[12] Ibid., para. 220.
[13] Ibid., para. 221.
[14] Ibid., para. 167.
[15] Ibid., para. 168f.
[16] In March 2024, the European Parliament and the Council agreed on two Regulations on Advance Passenger Information (API), Regulation (EU) 2025/12 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC, and Regulation (EU) 2025/13 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. The Regulations are aligned with the applicable rules for the processing of PNR data, as established in the PNR Directive. They take account of the interpretations made in the PNR Judgment regarding the processing of PNR data for intra-EU flights. Insofar as there is a possible overlap between the Regulation and the rules of the PNR Directive, the rules of the Regulation prevail, considering that it is both lex specialis and lex posterior. Article 13 of Regulation (EU) 2025/13 sets out specific criteria on how to select intra-EU flights if Member States decide to apply the PNR Directive and the API Regulation to intra-EU flights. The criteria mentioned are in line with the PNR Judgment as interpreted in this Statement.
[17] Ibid., para. 158ff.

that the application of the PNR system to intra-EU flights is limited to what is strictly necessary. In doing so regard must be had to the seriousness of the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons[18]. The main geographic connecting factor for the purpose of ensuring internal security is the EU.[19] The internal security of a single Member State is the minimum extent necessary.[20] Internal security in this regard has to entail the protection of life and safety of persons.[21]

16. Where a Member State is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, that Member State may collect PNR data of all intra-EU flights for a limited period of time.[22] However, the CJEU's Judgment needs to be read in full respect of the principle of (strict) necessity and proportionality. Thus, this principle is to be respected not only for the time of the application, but also for its scope (in particular as regards the selected flights, also geographically). Therefore, in case the threat does not extend to certain flights (e.g. categories thereof), the application to all intra-EU flights may not be necessary and proportionate. The respective authorities are obliged to make a proper assessment. This includes the investigation and consideration of facts and circumstances that may limit the scope of the application and thus of the interference with fundamental rights.

17. Especially smaller Member States with few airports may easily find themselves in a situation where the selection of intra-EU flights amount to cover practically all intra-EU flights, even in the absence of the said terrorist threat. This, however, would not be considered an indiscriminate application of the PNR Directive in the sense of paragraph 173 of the PNR Judgment if the necessary individual assessments have been made for the respective flights covered, including limiting the period of time and the scope of the application.

18. As the application of the PNR system entails substantive interferences with fundamental rights, all circumstances justifying the selection of the respective flights and the assessment thereof need to be documented properly and reviewed regularly, and also ad-hoc, to ensure that the application of the PNR system to intra-EU flights continues to be limited to what is strictly necessary.[23] In case of the broad application due to the said qualified terrorist threat, the decision providing for that application must be open to effective review either by a court or by an independent administrative body whose decision is binding[24], in other cases it is for the Member State to ensure such review.[25] Regular reassessments should be supported by an appropriate follow-up system (data protection by design) on the basis of the most current information available. This system should be automated, if possible. In case changes may already be expected (e.g. due to seasonality or dynamic developments), an appropriate resubmission period needs to be set. In case a condition leading to the cessation of necessity of the given selection is already definite, automated deselection of the flights or timely resubmission should be foreseen and safeguarded by an automated follow-up system. In case no changes are foreseeable, a regular resubmission should take place. A maximum resubmission period should be integrated in the system (data protection by default). As a general recommendation, the

[18] Ibid., para. 169.
[19] Ibid., para. 169; cf. also recital 15 of the PNR Directive.
[20] Ibid., para. 169.
[21] Ibid., para. 169.
[22] Ibid., para. 171.
[23] Cf. ibid., para. 172, 174.
[24] Cf. ibid., para. 172.
[25] Ibid., para. 172, 174.

reassessment should take place not later than six months after the last assessment; other periods may be acceptable if justified in the view of the specific circumstances. Moreover, ad-hoc review must be possible and its procedures should be reflected in the organisation (e.g. a contact point for reporting should be available). A fall-back maximum resubmission period needs to be provided for in that system, which, in general, should not exceed six months.

2.4 Data subject rights and automated processing

19. **The data subject rights referred to in Article 13(1) of the PNR Directive, and the right to judicial redress in particular, should be respected by providing comprehensive information (1) to the persons concerned, to be able to question the lawfulness of the automated processing and the following individual review, and (2) in the context of redress, to the court and the persons concerned, to examine the basis for the decision, i.e. the grounds and the evidence.[26] In both situations, certain exceptions to provide information may apply.[27] In order to properly balance the fundamental rights of the persons concerned and the interests of the competent authorities, the EDPB recommends that the competent authorities should establish clear and precise regulations, with proper procedural safeguards put in place.**

20. Article 13 of the PNR Directive provides for the data subjects' rights, including the right to judicial redress, by referring to the Law Enforcement Directive (LED). Article 6 of the PNR Directive entails the processing of PNR data, including by automatically comparing the data to relevant databases and predetermined criteria and the necessity to review any positive match individually. The recommendation aims to clarify how in particular the right to judicial redress may be guaranteed.

21. "*In order to call in question, as the case may be, the unlawful and, inter alia, discriminatory nature of the said criteria*", it should be "*possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress guaranteed in Article 13(1) of the PNR Directive*[28]. The CJEU finds that "*the competent authorities must ensure that the person concerned – without necessarily allowing that person, during the administrative procedure, to become aware of the pre-determined assessment criteria and programs applying those criteria – is able to understand how those criteria and those programs work.*"[29] This applies to the review criteria, as well.[30]

22. To further safeguard the right to effective judicial remedy, in the context of redress *"the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken […], including the pre-determined assessment criteria and the operation of the programs applying those criteria*."

23. In light of the foregoing, the EDPB is of the opinion that the interests of the competent authorities to limit the information provided in certain situations, must be properly balanced against the fundamental right to protection of personal data, including the right of the data subject to access to personal data, and the fundamental right to an effective remedy. In order to safeguard this, the EDPB recommends that the competent authorities should establish clear and precise regulations, with proper procedural safeguards put in place. The EDPB recalls that the competent authorities must also

[26] Ibid., para. 209-211.
[27] Ibid., para. 210f.
[28] Ibid., para. 210.
[29] Ibid., para. 210.
[30] Ibid., para. 210.

have regard to further in-depth guidance on the data subjects' right of access according to the LED that the EDPB is currently preparing.

2.5 Independent prior review

24. **A court or an independent administrative authority should perform the independent prior reviews. The independent authority that is entrusted with the prior review should be a different authority than the one involved in the conduct of the criminal investigation. Therefore, leaving the prior review to an independent officer or staff of a specific section *within* an administrative authority, that is not independent in itself, would in principle not be in line with what the CJEU Judgment envisaged in terms of independence. The same would apply to an independent officer or staff of a specific section within the authority involved in the conduct of the criminal investigation.**

25. The CJEU stated that "*it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority*"[31]. The recommendation aims to identify the elements that need to be in place to safeguard such independent prior review.

26. PNR data are data of a substantial number of air passengers. Most of these passengers have no link with terrorist offences or other serious crime. Access for law enforcement purposes should therefore be limited to what is strictly necessary so that fundamental rights are fully observed. PNR data are only accessible after prior review by a court or independent public body. To prevent the unlimited use of the data for the purpose of law enforcement, this independence is essential. According to the CJEU, independence means that the authority performing this prior review must:

- Be able to strike a fair balance between the interests at stake.[32]
- Have a status that enables it to act objectively.
- Be free from external influence and be neutral toward the parties involved
- Be a third party vis-á-vis the authority requesting access.
- Not be involved in the conduct of the criminal investigation.[33]

27. In addition, the EDPB points out that in order to be truly independent, this authority must also:

- Have sufficient resources, both in terms of budget and staff.
- Have sufficient knowledge in the field of law enforcement.

28. In light of the foregoing, a court or an independent administrative authority should perform the independent prior review. The EDPB stresses that the independence of this authority must be ensured and thus that the authority should be a different body than the one involved in the conduct of the criminal investigation. Therefore, it would not suffice in terms of independence to leave the prior review to an independent officer or staff of a specific section within an administrative authority, that is not independent in itself. Nor would it be sufficient if the officer or staff of a specific section within the authority involved in the conduct of the criminal investigation would carry out this review. Given the different organisational structures across Member States, implementation of this independent prior review may vary.

[31] Ibid., para. 223.
[32] Ibid., para 225.
[33] Ibid., para 226.

2.6 Retention period

29. **It is precluded to set a general retention period going beyond the initial period of six months. After the initial period of six months, individual PNR data sets may only be processed if for the respective data sets there is objective material capable of establishing a connection with the objectives pursued by processing under the PNR Directive, and only as long as it is necessary and proportionate[34]. Hence, the identification of objective material does not automatically lead to the maximum retention period of five years.**

30. According to Article 12 of the PNR Directive, Member States shall ensure that the PNR data are retained for a period of five years. However, the retention of PNR data pursuant to Article 12 cannot be justified in the absence of an objective connection between that retention and the objectives pursued by the PNR Directive[35]. The CJEU interpreted Article 12 of the PNR Directive in a way that the PNR Directive sets two distinct periods, the first being "*the initial retention period of six months*", and the other being "*the later period*"[36]. The CJEU clearly states that this distinction also applies to the requirement of an established objective link in order to justify the retention.[37] According to the CJEU, it "*is apparent from recital 25 of that directive, those provisions* [Article 12(2) and (3) of the PNR Directive] *reflect, on the one hand, the objective of ensuring 'that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations', which may be carried out already during the initial retention period of six months*".[38] The CJEU comes to the conclusion that during the initial period of six months, the retention may be justified to achieve such objective to use the PNR data for analysis and use in investigations.[39] "*By contrast, as to the later period, […] the retention of the PNR data of all air passengers […] runs counter to the requirement in recital 25 […] that the period during which those data are to be retained should be as long as is necessary for and proportionate to the objectives pursued*".[40] Further storage may be permissible only as regards PNR data of air passengers with an established connection between their PNR data and the objective pursued by the PNR Directive[41]; only in specific cases, in so far as objective material is identified, storage after the initial period seems permissible.[42] "*The continued storage of the PNR data of all air passengers after the initial period of six months is therefore not limited to what is strictly necessary*"[43]. Thus, the EDPB comes to the conclusion that providing for a general retention period in the laws of the Member States, going beyond the initial period of six months, is not permissible.

31. After this initial period, data may only be stored as long as necessary for and proportionate to the objectives pursued by the PNR Directive. The CJEU concluded that the identification of objective evidence according to which certain passengers may present a risk that relates to terrorist offences or serious crime is capable of establishing such a connection with the objectives of the PNR Directive. Hence, data retention may be justified during a period of five years[44]. Subsequent changes in circumstances (and the relevance of such objective evidence) that could change the outcome of the assessment of the necessity need to be considered and may lead to an earlier deletion. In case there

[34] Ibid., para. 259.
[35] Ibid., para. 251.
[36] Ibid., para. 252.
[37] Ibid., para. 254.
[38] Ibid., para. 253.
[39] Ibid., para. 255.
[40] Ibid., para. 256.
[41] Ibid., para. 254 in conjunction with 251; para. 257.
[42] Ibid., para. 259.
[43] Ibid., para. 258.
[44] Ibid., para. 259f.

is no positive knowledge that there is an objective link, there is no justification to store the information longer and the data need to be deleted. This also includes cases in which it is clear that no further analysis or investigation is set to take place. The assessment whether the continued processing of individual data is still necessary and proportionate to establish such a connection should be carried out regularly.

32. According to Article 13(6) of the PNR Directive, "*Member States shall ensure that the PIU keeps records of at least the following processing operations: […] The records shall be used solely for the purposes of verification, of self-monitoring, of ensuring data integrity and data security or of auditing.*" This means that the factor initiating the retention period for the respective record depends on the respective processing operation. Each record for a specific operation must be deleted five years after the start of the respective operation. Hence, the PNR Judgment only limits the term within which such operations may occur. Therefore, the retention period for records/logs and other documentation of five years is still valid.

3 FINAL REMARKS

33. The PNR Directive as interpreted and implemented before the PNR Judgment involved interferences with millions of data subjects across the EU, which the CJEU has determined were in parts not in compliance with the Directive. This highlights the urgency to aim for compliance with the requirements of the PNR Directive in the light of the PNR Judgment.

34. As far as the EDPB is aware, some Member States have started the adaption process but there is still a substantial lack of implementation efforts throughout the Member States. Therefore, the EDPB would like to underline the necessity for the Member States to adapt the practical application of the PNR system to the ruling of the CJEU in the PNR Judgment, but also to implement the restrictive interpretation set out by the CJEU by identifying and executing the necessary changes in their national laws. The EDPB has set out in this Statement some practical recommendations that in its view will need to be reflected in Member State laws transposing the PNR Directive in order to give effect to the findings of the CJEU in the PNR Judgment. This needs to be finalised in a timely manner.

35. The EDPB would like to refer to the responsibility of the Commission to monitor the implementation of the PNR Directive in national laws in conformity with the PNR Judgment. Moreover, the EDPB deems it necessary to ensure compliance of national laws and practice with the PNR Directive in light of the PNR Judgment. With this Statement, the EDPB intends to support the Member States in this important process. In case of incompatibility, national supervisory authorities reserve the right to take appropriate actions.

For the European Data Protection Board

The Chair

(Anu Talus)