Council of the European Union

Brussels, 9 September 2022
(OR. en)

11911/22

LIMITE

IXIM 200
ENFOPOL 428
AVIATION 199
CRIMORG 108

NOTE

From:	Presidency
To:	Delegations
Subject:	Improving compliance with the judgment in case C-817/19 – ideas for discussion

Delegations will find in the Annex a discussion paper on the abovementioned subject addressed to them by the Presidency.

ANNEX

This discussion document is intended to promote deeper understanding of the legal and operational consequences of the judgment of the Court of Justice in case C-817/19 and on the ways of promoting compliance by all the Member States; all deliberations and questions herein are intended to provide food for thought and stimulate discussion and, unless otherwise indicated, should not be attributed to particular subjects.

On the basis of the discussion of the judgment of the Court of Justice in case C-817/19 *Ligue des droits humains* (hereinafter "judgment") held at July IXIM Working Party, and on the basis of replies and suggestions of the Member States, the Presidency proposes to focus on following issues:

1. Intra-EU flights

It appears that there are strong operational reasons for continuing the application of the PNR Directive on intra-EU flights, even considering the limitations resulting from the judgment. Some Member States replied that about ¾ of their PIU workload represent cases involving intra-EU flights.

a. Flight selection

Many delegations pointed out that applying the system established by the PNR Directive to a selection of certain intra-EU flights only, presents a number of significant disadvantages. In light of that, it would be useful to explore any viable alternatives that might comply with the judgment. Pursuant to paragraphs 169 – 173 of the judgment, the collection of PNR data from *all* intra-EU flights may be justified only by a terrorist threat, which is genuine and present or foreseeable on the basis of sufficiently solid grounds. Such an indiscriminate collection of PNR data must be limited in time but the period may be extended if that threat persists. The judgment requires that such justification must be open to effective review by independent authority.

While the collection of PNR data from all or most of intra-EU flights would certainly avoid a number of operational problems, applying the PNR Directive in this way could only be considered sound if all or most of Member States could, before a court, justify as being sound their successive assessments that the terrorist threat each of them is confronted with is genuine and present or foreseeable.

1.a.i. Delegations are encouraged to evaluate whether this is a realistic premise, at least in their situation.

There are no other options concerning the selection of intra-EU flights explicitly identified in the judgment. It has been argued by some delegations, however, that the terrorist threat is not easily quantified and rarely limited to a specific time period. Effective limitation of processing of PNR data could potentially be achieved by "filtering" PNR data from all intra-EU flights by an automatic comparison with relevant databases (alerts) that lead to specific actions. In this "filter" procedure, false positives would be subsequently eliminated by feedback from the competent authorities or even verified by an independent body. It could be argued that as long as such processing retains only data on persons already actively sought by the law enforcement or judiciary and does not involve application of pre-determined criteria on or subsequent storage of personal data of other passengers, it does not apply *indiscriminately* to all air passengers.

1.a.ii.Delegations are invited to express their opinions on such filter. Would such a filter by appropriate if applied only to persons sought for terrorism or could it be applied for serious crime as well?

b. <u>Selecting intra-EU flights - technical, organizational, economic and operative issues</u>

When the collection of PNR data is limited to selected routes or airports, changes to selection of relevant flights must be expected, in terms of both air carriers and airports involved. This consequence of the judgment presents a number of challenges.

Technical challenges relate to the need to distinguish between the relevant flights (airports) within each air carrier data. Organizational challenges relate to the need to establish, activate and deactivate as necessary the data transfer relationships with relevant air carriers. These challenges would also be duplicated on the side of the air carriers in every Member State where they operate. Economic challenges are caused by increase of uncertainty in building PIU capacities, resources and data sharing relationships. Last but not least, a number of delegations pointed out that terrorists and criminal actors will seek out any information about selection procedures and results in order to undermine and circumvent the analytical and targeting functions of PIUs.

These challenges are inevitable to a certain degree, and indeed similar challenges are presented by long-term economic development (e.g. new routes), changing circumstances of air travel environment (e.g. new air carriers) and the mutable nature of crime and terrorism. However, Member States should discuss how any of the abovementioned issues could be further mitigated or addressed.

One potential mitigation option could be to limit the collection of PNR data through the action on the part of PIUs or other authorities, rather than through only limiting the transfer of PNR data by air carriers. This would require the PIU or other authority to delete – immediately and without any processing under Article 6 of the PNR Directive - incoming PNR data from flights or airports that have not been selected for processing for the applicable time period[1]. Consequently, the burden on the part of air carriers would not increase. The need to manage the ever-changing relationships to the air travel industry would remain at the current level. Most importantly, the current operative focus of PIUs would not be shared with the industry (and beyond). Obviously, strong safeguards would be required to ensure data is deleted correctly.

[1] Similar technique is used to separate PNR data from other incoming data in Article 6(1) of the PNR Directive.

Attention must be paid to ensuring that only relevant PNR data (based on the required assessments) are processed, because while the judgment sets clear requirements, it does not prescribe to the Member States how they must ensure these goals in law or practice[2]. It is also true that the judgment frequently (e.g. in paragraphs 165, 171 and 174) uses the term "transfer and processing". This may be interpreted as the obligation to limit the scope of the "transfer" from air carrier to PIU. However, the "transfer" is addressed here only in parallel with the "processing". It could be argued that the limits are intended to apply to the whole processing. In the same vein, paragraph 173 simply speaks about "application of the system established by the PNR Directive". The point 7 of the operative part of the ruling explicitly uses both sets of terms and does not consider "transfer" separately. In addition, the judgment accepts in principle (paragraphs 120 and 127) the protection afforded by prohibition of "processing" of sensitive PNR data in Article 13(4) of the PNR Directive.

1.b.i. What other challenges must be taken into account?

1.b.ii. What options do the delegations consider appropriate to ensure the application of the PNR Directive to intra-EU flights is limited?

c. Efficiency issues related to fragmentation of data collection

Concerns have been raised that the limitations set out in the judgment (on routes, on PNR data elements and on databases to which the PNR data may be compared) could result in reduced operational efficiency of PNR processing. In the context of flight selection, however, certain measures may help to avoid undesirable consequences.

One such practice could be for the Member States to allow their selection of intra-EU flights, airports and travel patterns be informed by the European-level threat assessment. With that in mind, Europol has been invited to present their activities related to PNR matters and to the threat assessment focused on air travel, as well as to discuss the added value of EU support to the Member States.

[2] This concerns both the part B.2.(c)(1) on which PNR data may be processed and the part B.2.(c)(4) on selection of flights.

Another possible way of cooperation could be for the Member States to be "mutually aware" of the risks assessments elaborated by other Member States. This could lead to focused discussion among Member States on the actual risks relevant for the internal security of the EU. Preferably, such risk assessments might be underpinned by a shared methodology or even by commonly accepted data sets.

In a certain number of Member States, the assessments may also be based on a multi-modal approach, i.e. by considering not only air travel but also sea and rail travel, or other modes of transport.

1.c.i. What other measures to improve the selection of intra-EU flights should be discussed?

1.c.ii. Would Member States be ready to share their risk assessments with other PIUs and to use the risk assessments established by other Member States? What would be the prerequisites and limitations of such an approach?

d. Exchange of PNR data collected from selected intra-EU flights

Article 9 of the PNR Directive provides for the exchange of PNR data and the results of processing of those data between the PIUs under certain conditions. This information exchange is initiated either by the PIU processing PNR data (on the basis of Article 6(2)) or by a reasoned request of other PIU. Article 2 of the PNR Directive allows the Member States to apply "all provisions of this Directive" also to some or all intra-EU flights. The judgment does not appear to modify this basic approach to the application of the PNR Directive. Therefore, it should be discussed whether it is possible for the PIU to share PNR data and results of processing of those data with other Member States, even if the relevant PNR data are derived from intra-EU flights, airports or patterns that other Member States did not (or could not) include in their own selection of intra-EU flights.

1.d.i. Do all delegations share this conclusion?

The judgment appears to require, in paragraph 224, that independent prior review of requests for the disclosure of depersonalized PNR data pursuant to Article 12(3)(b) is applied also to requests for the disclosure of PNR data in their original form (during the initial 6-months period). The aim mentioned by recital 25 to ensure the highest level of data protection has motivated this approach even though the recital explicitly excluded the initial period. It follows from the last sentence of Article 9(2) that it is the requested PIU which shall obtain prior authorisation of its own domestic independent authority.

1.d.ii. Do all delegations share this conclusion?

One of the practical challenges stemming from selection of intra-EU flights is lower level of reasonable certainty on the part of a given PIU that another PIU has access to PNR data required by the former. While PIUs could share their lists of selected flights (routes, airports and travel patterns), that might give rise to security risks. On the other hand, the handling of PIU requests for PNR data not collected by the requesting PIU may present significant administrative burden on both units.

1.d.iii What solution would be most appropriate?

This issue is connected with the frequency of a review of the assessment that led in the first place to the selection of a given set of intra-EU flights. The basic overview of the security situation in EU (in the form of the TE-SAT Report, the Frontex Report and the SOCTA review) is undertaken on an annual basis. However, air traffic is sub-divided into two main time periods (winter and summer seasons) each year. In addition, air carriers establish some routes, and close others, in a very short time frame. The correct level of granularity of an assessment is also important.

1.d.iv How frequently should the given selection of intra-EU flights be reviewed?

1.d.v Should the assessment allow the Member State to extend its selection of intra-EU flights where that Member State is taking account of the opening of a new route that shares the features of a route already selected?

e. Review of selecting intra-EU flights

In paragraphs 163 – 172, the judgment elaborates on the conditions that apply to the collection of PNR data from *all* intra-EU flights. Paragraph 172 clearly requires effective review by a court or by an independent administrative body for situations where all intra-EU flights are concerned. On the other hand, only paragraphs 173 and 174 deal with selection of intra-EU flights. Since paragraph 173 refers only to requirements set out in paragraphs 163 to 169, the independent review is not expressly included. Paragraph 174 requires the Member State to review the assessment of selected flights regularly, given the circumstances that motivated the selection of particular flights changes.

In both cases, the conditions applied seek to ensure that the processing remains limited to what is strictly necessary. However, the collection of PNR data on all intra-EU flights is substantiated by a single general evaluation that leads to a much greater interference with the privacy of individuals. As a consequence, the reasons for this extensive interference should be subject to independent review. On the other hand, the specific reasons that led to certain flights, airports or travel patterns being selected may differ from case to case. Changes in the circumstances that lead to that selection may simply imply gradual rather than systemic changes of the extent of data collection. Therefore, it appears that independent review is required for collection of PNR data when that collection is applied to all intra-EU flights but the Member States have more flexibility as regards review of their assessments leading to a selection of intra-EU flights.

1.e. Do all delegations share this understanding?

2. Retention of PNR data

The part E. of the judgment discusses the retention of PNR data under Article 12 of the PNR Directive. In paragraphs 252 - 254, a distinction between the initial 6-months retention period and subsequent 54-months later retention period is affirmed.

In paragraph 251, the judgment imposes further requirements on the later retention period[3]. Specifically, the judgment requires an objective link, even an indirect one, between retaining the data for the purpose of combating terrorism or serious crime and the carriage of passengers by air. Since the PNR data are retained in large quantities and their continuing retention would entail risk of disproportionate use and abuse, paragraph 256 refers to recital 25 to require further limitations on data retention to guarantee the principles of necessity and proportionality. Paragraph 258 explicitly forbids retention of the PNR data of all air passengers for the later period.

Paragraphs 257 and 259 of the judgment make a distinction between air passengers depending on whether or not they may be considered a risk that relates to terrorism or serious crime. The risk in question must be inferred from objective evidence, which may be produced by

a. the advance assessment under Article 6(2)(a) of the PNR Directive, resulting in verified positive match;

b. any verification[4] carried out during the initial 6-months period of data retention;

c. any other circumstance.

[3] On the contrary, paragraph 255 clarifies that for the initial period, retention of the PNR data of all air passengers is strictly necessary (because it allows identification of persons not originally suspected from involvement in terrorism or serious crime).

[4] The judgment presumably does not limit this term to verifications under Articles 11(2), 12(3)(b), 13(6) and 15(3(b) of the PNR Directive but possibly refers to any active processing of PNR data ("searches" in paragraph 255), in particular responses under Article 6(2)(b).

2.a What other circumstances could in practice present objective evidence of a risk? Could the PIU use new pre-determined criteria approved for future use even to re-assess already received PNR data (and stored for the initial period) to identify PNR data that should be retained for the whole 5 years?

Pursuant to paragraphs 257 and 259, and to point 5 of the operative part of the ruling, the risk presented by the air passenger must relate to terrorist offences or serious crime having a direct or indirect objective link with the carriage of passengers by air. While the requirement of "objective link" appears also in many other paragraphs of the judgment, only few places appear to provide further clarification.

In paragraph 155, examples of direct links between offences and air travel are given. These examples consist of terrorist attacks against aircraft, international travel in the course of terrorist activities, use of fake documents by human traffickers travelling by air, use of trafficked persons buying tickets with stolen credit cards to import drugs. In short, both offences targeting the carriage of passengers by air and offences committed during or through travel by air represent direct links. The indirect link is briefly elucidated in paragraph 156 which provides an example of air transport being used for the preparation of an offence or for evading criminal prosecution after committing such offences.

2.b What other examples of direct or indirect objective link may arise in practice?

In paragraph 220 the judgment interprets the words "sufficient grounds" in Article 6(2)(b) and "reasonably" in Article 12(3)(b) and makes a general comment that these words mean "objective evidence capable of giving rise to a reasonable suspicion" of a person's involvement in a serious crime". (Similar requirement is made in paragraph 204.) As regards terrorist offences, those requirements are satisfied when there is objective evidence from which it can be inferred that the PNR data could, in a given case, contribute effectively to combatting such offences.

Since the judgment requires these standards of evidence from all reasoned requests for access to retained PNR data (during both initial and later periods), it could be argued that the standards for mere retention of PNR data should be lower. The judgment appears to indicate as much by using the phrase "may present a risk" in paragraph 259 and by the word "risk" in point 5 of the operative part of the ruling.

However, it appears necessary to consider these very general requirements in terms of the practical functioning of the PIU.

2.c What other observations should be made?

3. Flights within the territory of a single Member State

The judgment does not explicitly address purely domestic flights. About half of replying Member States do not apply the PNR Directive to domestic flights or travel patterns, for various reasons (e.g. there are no domestic flights to cover). However, even the legal evaluation of such a measure differs among the Member States. According to some interpretations, the PNR Directive does not apply to purely domestic flights and the exchange of data derived from those flights may only happen through general channels of law-enforcement cooperation (such as SPOC). The definition of "intra-EU flight" in Article 2(3) and the wording of Article 2 of the PNR Directive support this interpretation. In addition, point 7 of the operative part of the ruling is based more generally on Article 3(2) TEU (on the area of freedom, security and justice without internal borders), Article 67(2) TFEU (on movement across internal borders) and Article 45 of the Charter (free movement and residence).

Elsewhere, paragraphs 167 and 175 of the judgment are based on Articles 7 and 8 of the Charter. It is not clear, in the context of protection of private and family life (Article 7) and protection of personal data (Article 8) whether the Member States should apply the rules for intra-EU flights also to domestic flights.

3.1 What is the position of delegations?

3.2 Is the application of the limitations in the judgment to purely domestic flights a material issue for delegations?

4. Criteria for selecting risk person

Part III.B.2.(c)(5)(iii) of the judgment deals with safeguards related to the automated processing of PNR data, in particular with use of pre-determined criteria by the PIU under Article 6. The judgment reiterates that both PIU (paragraph 203, for verification of matches) and competent authorities (paragraph 208, to prevent automated decision making in line with Article 7(6) of the PNR Directive) have to undertake individual review of PNR data. PIUs are to employ objective review criteria to focus the transfers of PNR data on relevant individuals and to ensure the non-discriminatory nature of using pre-determined criteria under Article 6(2)(a).

Paragraph 210 of the judgment requires that competent authorities ensure, without necessarily disclosing specifics, that the person concerned is able to understand how these criteria and assessment programs work. The purpose of this requirement is to allow the data subject to decide "with full knowledge of the relevant facts" whether to exercise the right to judicial redress against the possible unlawful (e.g. discriminatory) nature of such criteria.

On the basis of paragraphs 72, 73, 79, 80 and 83 of the judgment it seems clear that the LED[5] applies to processing of personal data by PIUs and competent authorities in the course of application of the PNR Directive. Indeed, the LED replaced the Framework Decision 2008/977/JHA to which Article 13 of the PNR Directive refers and references to this Framework Decision should be understood as references to LED.

[5] Directive 2016/680/EU

Consequently, the extent to which the information is available to the data subject and the application of various safeguards, such as the right to judicial remedy or the involvement of the data protection (supervisory) authority should be subject to the rules provided for by the LED (in particular, Articles 14 – 17, 54 and 56). Paragraph 210 of the judgment provides further guidance only in so far as to say that data subject need not be made aware of the specifics of pre-determined criteria or the programmes that apply those criteria but must be able to decide to exercise their rights with full knowledge of relevant facts. Point 1 of the operative part of the ruling does not cover this issue.

The extent to which information on data processing under LED is required or necessary for data subjects to initiate judicial redress guaranteed by the same is, incidentally, subject to a separate request for a preliminary ruling (proceedings in the case C-333/22 *Ligue des droits humains*) and further consideration of this topic might benefit from the replies and explanations given by the Court in those proceedings.

4.a What mechanisms could be employed to provide required information to data subject while avoiding prejudice to future deployment of criteria?

In addition, paragraph 211 of the judgment requires that the court reviewing the legality of decisions adopted by competent authorities, as well as the person concerned[6], be allowed to examine both all the grounds and the evidence on the basis of which the decision was taken, which includes pre-determined assessment criteria (but apparently not the objective review criteria under paragraph 206).

[6] Except in case of threats to State security.

Taking into account the applicable secondary law, it appears that the judicial remedies guaranteed to the "data subject" by former Article 20 of the Framework Decision 2008/977/JHA and by current Article 54 of the LED apply to breaches of rights related to protection of personal data. A set of requirements related to the judicial review of unspecified decisions taken by competent authorities pursuant to the laws of relevant Member State is likely included in the judgment due to prohibition of certain decisions (with adverse legal effects) pursuant to second sentence of Article 7(6) of the PNR Directive. Consequently, the information made available in the framework of such a judicial review should be such as to enable verification whether the second sentence of Article 7(6) of the PNR Directive has been complied with.

4.b What mechanisms and practices could be employed to provide required information to a person concerned without at the same time prejudicing the future application of pre-determined criteria?
