Council of the European Union

Brussels, 26 October 2022
(OR. en)

12856/22

LIMITE

IXIM 226
ENFOPOL 518
AVIATION 260
CRIMORG 144

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	11911/22
Subject:	Improving compliance with the judgment in case C-817/19 – comments from Member States

Delegations will find in the Annex comments received from Member States on document 11911/22.

ANNEX

Table of contents

AUSTRIA

1. **Intra-EU flights**

AUSTRIAN Position:

Since the decision was taken to stop the processing of inner EU flights (16/06/2020 non-extension of the national PNR Regulation), the AT PIU processes approx. 66% less PNR data than before. At the time the decision of disconnection of intra EU flights was taken, about 59 airlines were technically connected to the PIU (PNR/API).

Given the new circumstances, the PIU/at prioritized the connection of airlines that exclusively or predominantly serve destinations outside the EU from/to Austria. As of September 2022, 145 airlines have been connected. In terms of quantity, this means, the losses of data are significantly lower than in 2020.

Nevertheless, in AT - like in all EU MS affected by the recent judicial ruling - the accuracy of the PNR data evaluation instrument is (severely) limited in its effect, if intra-EU flights cannot be evaluated and analyzed appropriately. Intelligence gathered from the area of state protection and the OC area confirms this. (Example: According to findings in the field of counter-terrorism, a member of AL KAIDA was supposed to travel from EU country X to AT. The verification of whether the person did actually board the flight was only possible through the costly use of personnel and time resources (including airline and airport personnel). If the check via PIU would have been possible, a corresponding clarification could have been issued in no time. The added value in the case of an imminent terrorist threat is obvious. It is known that members of terrorist cells located in Europe maintain extensive cooperation with members of other terrorist cells and pay visits to each other by air. Additional examples from the field of counter-terrorism as well as from the field of criminal police are known and available on demand.

a. Flight selection

AUSTRIAN Position:

According to the ECJ judgement, processing of INTRA EU flights is only possible, if the MS could highlight concrete and real terror related threats. In the majority of such scenarios the immediate threat to a country will not be possible to be determined on an ad hoc basis. In addition, it is unlikely that a national competent authority will be able to provide such an extensive analysis of the situation in a timely manner. Furthermore, PNR data cannot be provided by an airline to the respective PIU by activating a button. Technical adjustments in accordance with valid data protection regulation, settings in several IT systems needs to bet activated, tested, validated before a regular data flow can be agreed. To this end we would highlight that the use of PNR data is an important prevention tool to identify terrorist attacks before the happen.

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

AUSTRIAN Position:

The possible technical implementation of such filter mechanism, as well as the legal possibility in the light of EUGH judgment, needs to be discussed in more detail.

Another possibility for the processing of INTRA EU flights is to use the national terror warning level instrument as an indicator. For example, if the scope of the threat level range from 1-5 (1 low level-5 highest level) Level 3 is activated, all INTRA EU flights need to be processed until the level will be downgraded to Level 2.

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?

AUSTRIAN MOI/Statement

See above answer.

b. Selecting intra-EU flights - technical, organizational, economic and operative issues

AUSTRIAN Position:

It will be not actionable to react as a PIU within a short timeframe on changed conditions like particular flight routes, airports or airlines. The data transfer requires complex data settings, in accordance with strict data protection components, on both sides, the Airlines IT environment and the PIU IT environment. The data transfer cannot be activated and disabled by pressing a button. Complex system settings and regulations need to be agreed to from both sides, which cannot be realized within a short timeframe and reverted back to if the situation changes again.

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

AUSTRIAN Position:

The undertaking of an airline requires multiplicity of organizational, technical as well as legal necessities. If the single airline (small Carriers) will now be confronted to change their settings according to changed situations in the various MS, we assume that this will not be feasible for several Carriers. In addition, and already explained in a former paragraph *ad hoc* changes in the technical, secure environment for the data transfer and communication cannot be handled in a short timeframe and then changed ,if the situation in the country changes. The connectivity of an airline to the AT systems requires multiple organizational and technical steps. As for AT experience after the connection of 145 Air Carrier so far, these processes - from the beginning to the final connectivity - last from one week up to several month. To be in line with the data protection regulation, all the data needs to be processed in a highly secure, isolated IT area. It will be not feasible to activate and disable such settings on a daily basis and according to the current situation.

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

AUSTRIAN Position:

The use of a European Threat Assessment (TA), such as TESAT or SOCTA is to our opinion not convenient. Those TA are based on European Union findings compiled throughout the previous year, thus retroactive and cannot highlight the current state of play in the respective MS. But the use of a common agreed terror warning level (see 1.a.i, Level 1-5) for the possible use of INTRA EU flights seems to be a feasible way.

c. Efficiency issues related to fragmentation of data collection

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

AUSTRIAN Statement:

The restriction to certain flights, airports or routes, based on the decision of a single EU member state will not be feasible - both technically and organizationally. Furthermore, the original purpose of the Directive, as confirmed by the ECJ, is massively limited and would lead to a weakening of the European security architecture. In a new/adapted EU Directive after the ECJ ruling, a binding possibility for the processing of INTRA EU flights should therefore be determined in a well-considered manner and in a solution that is coordinated with the EU Member States. From an operational point of view this could be best achieved through a legally binding act in the form of a PNR Regulation. It has to be stressed however, that all rules of data protection have to be upheld and that any new legal text will not serve as a vehicle of circumventing the ruling of the ECJ.

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?

AUSTRIAN Position:

The exchange of PNR data is not affected by the ruling and is sufficiently determined in AT by the PNR Act (PolKG). The possible exchange of threat analyses does not appear to be appropriate, since the underlying data were considered and analyzed on a national basis. Concerns are also raised here with regard to state police/intelligence practices. It should be noted that according to the PNR Directive (Art. 9(2), in "case of need") and the ECJ, data transfer between the individual MS appears to be permissible only on a case-by-case basis. In our view, the transfer of all PNR data on intra-EU flights of another member state does not appear permissible.

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

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

AUSTRIAN Position:

Independent prior review, even for "normal" data sets, when forwarded to a requesting PIU is sufficiently elaborated, also with regard to data protection components.

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

AUSTRIAN Position:

From a practical point of view, the described exchange of "lists" does not appear to be feasible from an organizational point of view, nor does it appear to be tenable from a data protection point of view, nor does it appear to be expedient. The selected routes, airports, and airlines were created and agreed upon on the basis of specific national analyses and cannot be transferred unisono into another country.

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

AUSTRIAN Position:

In order to be accurate, a concrete, targeted assessment would have to be carried out at regular (short) intervals on the basis of governmental/ intelligence and international findings. Even if such an analysis were available (unrealistic), it would not be feasible from a technical and legal point of view for the airlines. They were not able to react to the changed situation at short notice and provide the required data (even if a technical connection already exists!).

An assessment can therefore only be made at the national level with the involvement of the authority responsible for state protection tasks for the respective country. The state protection interest of the respective country should form the arguable basis whether the processing of PNR data from Intra EU flights is necessary and therefore justified.

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

AUSTRIAN MOI/Statement

See answer to previous point

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?

AUSTRIAN MOI/Statement

See answer to previous point

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

AUSTRIAN MOI/Statement

See answer to previous point

2. Retention of PNR data

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?

AUSTRIAN Position:

The review of PNR data already received could be carried out by means of criteria considered in advance and approved for future use. But such creation of criteria is technically difficult to implement, as it would have to take into account all three collection variants (prior review pursuant to Para. 6(2) PNR Directive, any other review or other circumstances (before the expiry of the 6-month period). Uniform criteria, binding on all member states, should be established to guarantee legally compliant PNR data retention.

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

AUSTRIAN Position:

Direct examples of an objective connection, such as terrorist attacks on airplanes etc., are obvious. But indirect objective connections concern any acts of prevention of a crime or escape from prosecution, as already mentioned in para. 156 of the ECJ judgement. The boundaries of whether criminal acts have an indirect objective connection are fluid and require a precise delimitation/interpretation by the Directive editor. In particular, to avoid the risk that terms such as "sufficient" etc. are interpreted differently by each member state. Also in this respect, any new legal act (may it be a Directive or a Regulation) will need to provide sufficient legal certainty.

2.c What other observations should be made?

AUSTRIAN Position:

See answer to previous point

3. Flights within the territory of a single Member State

3.1 What is the position of delegations?

AUSTRIAN Position:

The PNR Directive is not applied to flights within the territory of AT.

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

AUSTRIAN Position:

The application of the Directive to domestic flights was already excluded for AT in the project phase. Due to the geographical conditions and the number of domestic flights in question, it is unlikely that a modified (EU) Directive will cover them.

4. **Criteria for selecting risk person**

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

AUSTRIAN Position:

By disclosing the considerations, there is a risk that criminals will adapt their travel route in advance in order to avoid any possible hits. How broadly or narrowly this information must or may be defined requires a precise definition by the Directive Editor. In this regard, the outcome of the separate preliminary ruling (Case C-333/22), which is already pending, should be awaited.

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?

AUSTRIAN Position:

See answer to previous point

BELGIUM

- Belgium fully recognizes the importance of the collection of PNR for intra-EU flights. It calls upon Member States to explore all options or solutions to comply with the Court ruling on PNR without losing crucial travel information : from a coordinated risk assessment approach (short term) to regulating the intra-EU collection with a new legislative act (middle term), the latter providing for clarity and uniformity.

- According to its first assessment, Belgium would not be able to use its terrorism threat level as instrument to justify the generalized intra-EU collection (currently on a level 2 of 4). Moreover, this seems a very unpredictable solution as threat levels may change over time and may be different from member state to member state, leading to fragmentation of data collection.

- In case of specific routes to be collected, Belgium supports the idea of having a filter at member state level, meaning the carrier should not be made aware of the choice the Member State has made on the basis of its risk analysis.

- Belgium reiterates its position to call upon the establishment of an expert working group under a Council structure (IXIM or other) that would be tasked with the development of a risk assessment methodology and the execution of it, in order for the member states to work collaboratively on the motivation of the necessity to collect information for a large majority of intra-EU flights.

- Risk assessment(s) should include a.o. following criteria :

    - The waterbed effect : criminal phenomena may shift to other destinations. Hence, the collection of data for flights from/to neighbouring countries can be motivated.

    - Experience (qualitative and quantitative data) of the past for all destinations (e.g. number and type of hits).

    - As one of the purposes of the Directive is about the 'detection' of terrorism and serious crime, destinations for which no historical data is available should be taken on board and re-assessed once sufficient data is available.

    - The mutual recognition of risk indicators/assessments, the sharing of data where possible, needed and relevant.

    - The use of existing and future risk assessments done by EU agencies such as Europol and Frontex.

- Risk assessments should be conducted every 6 months and, where needed, on an ad hoc basis.

- Risk assessments should also include criteria to argue for the need to store and use data for specific routes for a period up to 5 years.

CYPRUS

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

According to the Court ruling, the optional application of the Directive to intra-EU flights must be curtailed. Application to all intra-EU flights is only possible if a Member State is confronted with a genuine and present or foreseeable terrorist threat. In the absence of such a terrorist threat, the application of the Directive to intra-EU flights must be limited to certain routes or travel patterns or to certain airports for which there are, at the discretion of the Member State concerned, indications that would justify that application. In addition, this is flanked by the procedural requirement that the extension of the application of the PNR Directive to selected intra-EU flights is subject to effective review, either by a court or by an independent administrative body.

It therefore appears that Member States can use both methods provided by the Court, according to that Member States specific circumstances. Specifically, if according to a national risk assessment, there is a genuine and present or foreseeable terrorist threat, then the processing of data from all intra-EU flights would be considered permissible, until the national risk assessment demonstrates that the aforementioned threat no longer exists. If the national risk assessment does not demonstrate such a threat, or if it demonstrates such a threat but the origin of the threat can be identified beyond a reasonable doubt (e.g. connected to a passenger arriving from a specific route or airline), then that Member State confronted with such threat may not process data from all intra-EU flights but only from that route or airline. Therefore, the method to be used by the Member States depends on the individual circumstances of that Member State.

Moreover, in our opinion, in the case where, following a risk analysis by an EU Agency or following information in the possession of an EU Agency, the possibility of a terrorist threat within the EU is high, without however being able to determine beyond a reasonable doubt, which Member State may be affected by the terrorist threat, then all Member States, on the basis of said risk analysis or information, can process data from all intra-EU flights until the terrorist threat seizes to exist.

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?

The issue that arises in this situation is whether the filtering of all passenger's data on all intra-EU flights, constitutes processing of personal data in accordance with the GDPR and the LED. Article 2 of the LED provides the following definition of processing: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. If the filtering process mentioned above falls withing the definition of processing, then we must first assess whether it is in line with the LED and the Court Ruling, even if all the data are not to be stored.

In case it is not considered processing or in case it is considered processing but it's in line with the LED and the Court Ruling, then in our opinion the filtering process will not be adequate for the purposes of the PNR Directive as it would not allow the identification of persons that constitute a terrorist threat or are linked to organised crime and who are not already in relevant databases. Moreover, the application of such a filter will produce a lot of challenges concerning the simplification and harmonization of EU policy and will generate an excess load on the administrative procedures of air carriers.

As the Court ruling does not preclude the processing of PNR data against pre-determined criteria, our opinion is that such practice should continue but ways should be sought in order for such pre-determined criteria to be in line with the Court's guidance.

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

We agree on the challenges identified by the Presidency and further stress that the economic impact on the Member States (e.g. for modification of the national software) should also 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?

The selection of intra-EU flights should be based on predetermined criteria established following risk assessments produced by Member States. The said risk assessments should be conducted on a regular basis in order to allow the predetermined criteria to be regularly reviewed.

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

We agree with the Presidency's proposals on both to allow the selection of intra-EU flights, airports and travel patterns be informed by the European-level threat assessment as well for the Member States to be "mutually aware" of the risks assessments elaborated by other Member States. Furthermore, we would also like to emphasize on the formation of a unilateral approach regarding risk assessment, by developing a common risk analysis model applied by all Member States.

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?

Yes, we would be ready to share our risk assessments with other PIUs and to use the risk assessments established by other Member States. We do not identify any additional prerequisites or limitations and are in favour of applying the ones already applicable, under the legal framework for the exchange of PNR data between MSs and Europol.

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

In our opinion it is possible for a PIU to share PNR data and results of processing of those data with other Member States, even if the relevant data are derived from intra-EU flights, airports or patterns that the other Member States did not include in their own selection of intra-EU flights, provided that the conditions of article 6(2).

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

Yes we also share the aforementioned conclusion. However, we should bear in mind that the national independent authorities and Courts do not operate on a 24/7 basis and this could lead to additional delays in terms of responding, something that could potentially have a negative impact on urgent requests.

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

Law Enforcement Cooperation is on a high degree based on trust between Member States and therefore we are in favour of sharing the lists of selected flights between PIUs, provided that the sharing will be made through a secure communication channel. Implementation of a platform that would indicate in real time or ad hoc the data collected is highly recommended.

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

As mentioned in previous answers, the selection of intra-EU flights should be based on regular risk assessments conducted by Member States. The said risk assessment should be reviewed regularly (every month), in order to allow the review of the selection of intra-EU flights. Moreover, we propose to consider the establishment of a working group, composed by Heads of PIUs which will meet on a monthly basis in order to assess and review the need for the selection of intra-EU flights.

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?

The routes to be selected should be assessed individually and on a case by case basis, in order for the Member State to be able to provide sound justification when necessary for the selection of the relevant routes. However, it could be taken into account as a possible indicator, for criminal routes that share similarities and /or features. We propose that this issue be discussed during the meetings of the working group proposed in answer 1.d. iv.

1.e. Do all delegations share this understanding?

Yes we share this understanding.

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?

The Decision of the Court does not elaborate on what other circumstance may reveal the existence of objective evidence capable of establishing a risk. Since the same wording has been used in the Opinion 1/15 of the Court on the EU-PNR Agreement, perhaps we could draw guidance as to how it was interpreted in that context.

In order to comply with the Decision of the Court, PNR data already obtained should be re-assessed based on specific criteria to be established by the Member States. Should the aforementioned filtering process (circumstance), indicate objective evidence of risk, then the retention of the said data should be retained for the whole 5 years.

3.1 What is the position of delegations?

As regards Cyprus, there are no internal flights.

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

As regards Cyprus, there are no internal flights.

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

We share the conclusion that the LED is applicable as regards the processing of data in the context of the PNR Directive and thus 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. The extent of the information to be provided to the data subject should be limited to what is strictly necessary to comply with the judgement of the Court and in order for the data subject to be able to decide to exercise his rights with full knowledge of relevant facts. To establish what mechanisms could be employed to provide required information to the data subject, while avoiding prejudice to future deployment of criteria we must establish the extent of the information to be provided to data subjects. Therefore, the issue should be discussed following the court ruling in the aforementioned case.

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?

See answer in 4.a.

DENMARK

1.a. ii.)

The concept of filtering all PNR and API data is currently incorporated in the daily PIU activities. The PIU has made a collective and conscious point in the creation of the Danish PIU, to focus purely on relevant data for investigations and the apprehension of serious criminals and terrorists.

The PIU utilize the same filter in both our terror and serious crime cases. The filtering in practice functions through cross-referencing criminal databases and the utilization of rules and watch-lists, which bring to focus the passengers most likely worthy of greater scrutiny.

If the legal basis for the filter suggested in the text excludes rules and watchlists, and the filter would only be based on cross-referencing databases (automatic comparison) this will definitely limit the effectiveness of the process. When considering such filter as a solution the general data quality of PNR-data must be taken into consideration.

1.b.i.)

The Danish National Police agrees with the statements that terrorists and criminals will quickly find the data gaps or routes that we are not monitoring to avoid border control and surveillance. Determining relevance of some routes over others prior to unforeseen criminal and terrorist activity would prove to be a difficult task. This would likely have a very reactive affect to the PIUs current proactive workflow.

1.b.ii.)

The Danish National Police does not see any appropriate or useful options to minimizing intra-EU flight data. However, the Danish National Police agrees that if and only if data should be removed, then it is best left up to the national authorities and not the airlines to minimize technical and financial burdens on an already stressed industry. Secondly, informing airlines and handlers of uncollected routing would almost be equivalent to posting activities and knowledge on the internet.

This means that if the airlines are tasked with only pushing data for certain routes determined by national authorities on the basis of risk assessments, this information must be regarded as public knowledge. This will have an adverse effect on the possibilities to write up risk assessments, as the information therein or at least the conclusions (i.e. the routes selected for information) will be made public.

1.c.i.)

At present, the The Danish National Police does not see other relevant measures to improve the selection of intra-EU flights. It is very difficult to point out a logical methodology for removing data from a pool in which unforeseen future events have yet to play out.

1.c.ii.)

As a starting point The Danish PIU will be prepared to share risk assessments with other PIUs and to use the risk assessments established by other Member States. However, it is difficult at this stage to devise the framework, methods and requirements for such risk assessments, as this depends on many unknown factors, i.e. the level of openness to the public or the airlines and if the assessments should be been subject to review by an independent authority.

Currently Danish PIU is active with sharing risk assessments in the form of PNR Rule sharing and serious crime seizure statistics, which could be utilized for selection of activities. However, most member states PIUs find their risk assessments highly sensitive and of national security. If this current practice will also be characteristic for sharing risk assesments with regards to collecting PNR from intra Schengen routes, this may present a challenge.

Limitations may arise in the geography, socioeconomics and societal norms, from country to country. Each country can share their assessments, but could have little or no effect for other countries.

1.d.i.)

If the legal basis for collecting PNR-data from specific routes is present in one Member State but not in another Member State the data should be transferred if the legal basis for the transfer is established.

1.d.iii)

Solutions regarding sharing of risk assessments may course an enormous administrative burden on the PIUs. If the data were not accessible or collected for one Member State's PIU, the other Member States would quickly discover the deleted routes or missing data through declined PIU requests. The number of PIU requests would theoretically explode as a method to avoid or circumvent the lack of routes or data found in each national system. At present, the Danish National Police is not able to point at relevant solutions.

1.d.iv.)

Routes and carriers change almost monthly, so review frequency would be of great importance. Risk analysis based on an ever-changing transport industry generates necessity for a daily or weekly review and analysis. This would have a direct workload effect on every PIU.

1.d.v.)

As such a route would be an alternative for travelers using the already assessed route the assessment should be extended to new routes sharing the features of a route already selected.

2.a.)

The Danish National Police is at present not able to point at other circumstances that could present objective evidence of a risk.

2.b.)

Depending on the specific circumstances of the offence in question, most serious crimes included in the directive may possibly have a direct or indirect link with the carriage of passengers by air. The answer to this question is, at the end, linked to interpretation and limitation of the words "indirect link".

ESTONIA

- Due to our geographical location we don't see the possibility to exclude even partial collection of regular intra-EU flights. Most passengers are coming to Estonia using other airport hubs in Europe. We never know which route or airline will be used by the criminal organizations.

- The decision of the European Court of Justice is still under analysis phase on the national level. At the first findings, all intra-EU data collection consequently from the foreseen terrorism threat is not feasible in our case. Even if such situation arises, it will be a temporary solution and does not cover long-term needs of MS-s. Besides, the situation of other EU countries should be taken into account, as the PNR is not only the national tool for combating serious crimes and terrorism, but also a mechanism that provides high value due to cooperation and PNR information exchange between PIUs.

- Intra EU data filtering based on risk assessment should be done on the PIU level. Otherwise there is a serious threat of information leak. Furthermore, this situation causes a problems to aviation industry, because there will be no clear requirements by the country regarding PNR data transfer.

- It is necessary to form a clear distinction of "collection" and "proceeding" terminology in the view of the judgment. It should be general position to all EU level data retention related legislation. Some legal analysis should be made concerning this issue, PIU DPOs could be also involved.

- Opinion of the European Court of Justice significantly changes PNR data processing by the PIUs and brings about to the member states basically in all areas (legislative, workflow, PIU staff competence and IT developments). Thus changes bring additional costs to member states, particularly resources and fundings. This problem should be also highlighted on EU level.

- And finally Estonia fully supports Belgium delegation proposal to establish separate working group, which should consist of practical and legal field experts and whose mandate is to deal within the decision of the European Court of Justice, incl. finding out possible solutions. PNR data processing should be harmonized on the EU level otherwise we will be in the situation, where different member states implement their own interpretation of the judgment.

FINLAND

1. **Intra-EU flights, relevance;**

There are strong operational reasons for continuing the application of the PNR Directive on intra-EU flights, even considering the limitations resulting from the Directive and the judgment. Finland is in the same situation as many other Member States, with around ¾ of the workload of the PIU focus to the intra-EU flights. This year (2022) 81% of PNR data transfers have been related to intra-EU flights. Needs for all intra schengen PNR data is critical for Finland.

a. Flight selection;

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

The collection of intra-Schengen PNR data is critical for Finland. From an operational point of view, the system established by the PNR Directive to a selection of certain intra-EU flights only (flight selection), presents a number of significant disadvantages. However, not only the judgment, but also the Directive does impose certain limits. We should explore how to find a solution allowing the collection of intra-Schengen PNR data so that critical operational needs are responded to, and at the same time analyse what the Directive and the judgment require in practice."

Judgment paragraph 169; The Member State shall ensure that the processing of PNR data is limited to what is strictly necessary. Attention must be paid by Member State 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.

Pursuant to paragraphs 169 – 173 of the judgment, the processing 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, and for a limited period of time. We should explore to what extend the judgment really require need for flight selection or selection of data for PNR processing.

In generally, we may say that the terrorism threat in Finland, threat against national security and sovereignty just now really persists. We agree that an indiscriminate processing of PNR data in Intra-Schengen traffic must be limited. The judgment requires that such justification must be open to review by independent authority.

In Finland, the levels of terrorist threat are divided into four levels: 1. low, 2. elevated, 3. high and 4. very high. The current threat is level 2. elevated. As an interpretation, this level 2 elevated level may be considered to allow the application of the Directive to the Court of Justice, as required, for all intra-EU flights departing from or arriving in Finland, for a strictly necessary limited period (as long as level 1 is restored).

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?

With reference to the previous question (1.a.i), in case of specific routes to be collected, Finland supports the idea of having a filter at member state level, meaning the carrier should not be made aware of the choice the Member State has made on the basis of its risk analysis. National legislation does not allow disclosure of tactical and technical methods by law enforcement authorities.

The extension of the PNR Directive to intra-EU flights will be limited to what is strictly necessary to achieve the objective in the PNR process in the PIU, in accordance with the requirements set out in paragraphs 163 to 174 of the Decision (paragraph 285 of the Decision).

Would such a filter by appropriate if applied only to persons sought for terrorism or could it be applied for serious crime as well? Based on PNR directive recital point 19; Each Member State should be responsible for assessing the potential threats related to terrorist offences and serious crime - we see that terrorism and serious crime should be applied together.

b. Selecting intra-EU flights - technical, organizational, economic and operative issues;

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

Like the discussion paper says selection between the most relevant routes is impossible, if that is done, like pointed out in paper, 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.

The burden on air carriers should not be increased or imposed on them to modify their procedures on a monthly or other basis within a short period of time. The management of relations in the air transport sector must be stable. Air carriers will carry out their PNR obligations in the same way under all circumstances. Member States shall ensure that only relevant PNR data (based on the required assessments) are processed.

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

Attention must be paid by Member State 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.

c. Efficiency issues related to fragmentation of data collection;

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

One good practice could be that Member States allowed their selection of intra-EU flights, airports and travel patterns to be informed for the European-level threat assessment. Member States should be "mutually aware" of the risks assessments elaborated by other Member States.

Extra-EU PNR handling procedures should be equal at in every MS and cover for all traffic modes. Even then we should not leave Intra Schengen traffic unattended without interactive control. Terrorism is a planned activity, it is concealed and it exploits the institutions, assistants and actors already in the EU. The best and most up- to-date information on terrorism is the responsibility of national authorities. They should be more and more involved in the handling of PNR. In Finland the assessments 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.

Other measures include enhancing the possibilities for exchanging information, in particular the technical implementation of the exchange of information, in the ways already provided for in the PNR Directive.

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?

National legislation allows us to majorly share and use of risk assessments established by other Member States (when those fits for our national risk assesment framework).

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

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

Yes, when we speak so called spontanious exchange, It is possible for the PIU FI 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. It is indispensable to be able to share PNR data and results both on request and by own assessment, if the data can be considered relevant and needed by the recipient.

1.d.ii. Do all delegations share this conclusion [paragraph 224, independent prior review of requests for the disclosure of depersonalized PNR data] ks.

Yes; 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). PIU shall obtain prior authorisation of its own domestic independent authority.

1.d.iii. What solution would be most appropriate [intra-EU flights risk level anomalies] ?

See:1.b.ii Airlines will send all PNR data and attention must be paid by Member State 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.

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

If there is a selection needed, reviewing should be done continously together with competent authority. The air traffic may be sub-divided into two main time periods (winter and summer seasons) each year, but we must notice also winter time holiday seasons and specially totally new routes. New carriers come and new routes are opening and and also closing all the time. Opening new routes are often tested by active crime groups, due they think authorities are not yet aware criminal use or ready with passenger monitoring tools. Anyway we may say that criminals travel all the time as do the normal business man, even during covid-19 when business travelling were majorly on hold.

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?

Yes; New carriers come and go and new routes are opening and and also closing all the time. The lack of relevant information is important element to take account of risk analysis implementation; As one of the purposes of the Directive is about the 'detection' of terrorism and serious crime, destinations for which no historical data is available should be taken on board as full and re-assessed once sufficient data is available.

e. Review of selecting intra-EU flights;

1.e. Do all delegations share this understanding?

That is a good point that collection of PNR data on all intra-EU flights is substantiated by a single general evaluation that may lead 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.

It's clear that In a paragraph 172 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, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists. The conditions applied seek to ensure that the processing remains limited to what is strictly necessary.

Again; 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. Retention of PNR data

According to the decision, the general five-year retention period should not apply to all passenger data. Inspection carried out during a six-month period or other facts have revealed objective evidence which would indicate a link between a passenger's flight and terrorist offenses or serious crime (the link between passenger air traffic is required in the context of both terrorist offenses and serious crime in paragraphs 257 and 262 of the Decision, which deal with this particular issue).

The retention of data must be limited to what is strictly necessary. For other passengers, the retention of data for a period of more than six months is not strictly necessary. Their data shall be subject to a general retention period of six months.

According to the Court, the six-month retention period does not seem to exceed what is strictly necessary, as it allows for searches to identify persons who were not previously suspected of involvement in terrorist offenses or serious crime.

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?

PIU may processing PNR data only based on PNR directive article six (6.2.a,b,c). Carrying out an large and automatic assessment of passengers prior to their scheduled arrival in or departure from the Member State only.

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

The Court also states that offenses which have no direct connection with passenger air transport may nevertheless have an indirect link with passenger air transport on the basis of the circumstances of the individual case. This is particularly the case when air transport is used as a means of preparing such offenses or avoiding prosecution after they have been committed. Apart from these, there are crimes which have no objective connection, even indirect, to air transport by passengers, and these should not be subject to the system established by the PNR Directive. (Paragraph 156 of thedecision). This leads to the conclusion that the indirect link can be considered to be established in a number of different ways, and only cases not strictly related to passenger air transport are excluded from the scope of the directive.

2.c What other observations should be made?

Paragraph 259; However, in so far as, in specific cases, objective evidence, such as the PNR data of passengers which gave rise to a verified positive match, is identified from which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime, it seems permissible to store their PNR data beyond that initial period.

Uniform interpretation for 'may present a risk' (determination) would be beneficial.

3. Flights within the territory of a single Member State;

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?

Agree - domestic flights PNR is not in use in Finland, due PNR directive 3. article 2.and 3. determination.

4. **<u>Criteria for selecting risk person;</u>**

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

The controller shall maintain a written record of the processing of personal data under its responsibility, which shall be made publicly available.

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?

The main weight in the criteria and evidence to be disclosed should be contained in material enabling the legality of the decision to be assessed and in evidence of possible discrimination or non-discrimination.

Comment on improving compliance with the judgment in case C-817/19 context;

Finland support Belgium's call for the establishment of an expert working group under a Council structure (IXIM or other) that would be tasked with the development of a risk assessment methodology and the execution of it, in order for the member states to work collaboratively on the motivation of the necessity to collect information for a large majority of intra-EU flights.

GERMANY

In Germany, we have not yet completed our analysis of the ECJ's judgment. We are therefore only able to provide preliminary assessments in response to the questions raised by the Presidency. It remains to be seen what the result of the further discussions in Germany's Federal Government will be.

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

1. As Germany understands the ECJ's judgment, it is the responsibility of the Member State concerned to assess whether there are "sufficiently solid grounds for considering that [it] is confronted with a terrorist threat which is shown to be genuine and present or foreseeable"; it is not necessary for all the Member States to arrive at the same assessment at the same time. . This is how Germany understands paragraph 171 of the judgment. The period in which such an assessment is valid may be extended. However, in view of the requirements which the ECJ has specified and which are specifically intended to end the possibility of applying PNR mechanisms to all intra-EU flights and limit the processing of PNR data to the absolute minimum necessary, it is unlikely that permanently extending the assessment would meet the ECJ's requirements. In Germany's view, the ECJ's requirements for processing data from intra-EU flights raise in particular the question of how the Member State confronted with a terrorist threat will be able to process such data for a limited period of time.

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?

- As Germany understands it, a filter that is the equivalent of a regular check of the registers would not meet the ECJ's conditions, because the PNR data of all passengers would be subject to such a check and would then be processed in the PNR system.

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?

- According to our initial examination, under the current technical conditions it is necessary for purely technical and operational reasons for air carriers to be permanently connected to the PNR system in order to be able to temporarily process flights to or from the Member State where the terrorist threat exists. If no terrorist threat has been ascertained or if no threat assessment for the route concerned exists, the data supplied must then be automatically deleted immediately. However, according to paragraphs 92 to 97 of the ECJ's judgment, all processing covered by the PNR Directive, including the transfer of PNR data by air carriers to the passenger information unit (PIU) of the Member State concerned, constitutes interference with the rights guaranteed by articles 7 and 8 of the EU Charter of Fundamental Rights. Further legal analysis is needed to determine whether the ECJ's decision would also bar the ongoing transfer of data that would then be immediately and automatically deleted.

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?

- Terrorist threat:

We are still in the early stages of considering issues related to assessing a terrorist threat situation. Depending on the results, Germany will also examine possibilities for sharing risk assessments with other Member States. Whether the risk assessments of other Member States are applicable to the terrorist threat in Germany will depend on the threat situation in question and will have to be examined in the individual case with attention to the applicable law. It should also be noted that each Member State must conduct its own risk assessment and cannot use other countries' risk assessments without further examination.

- Certain routes or travel patterns or certain airports:

Germany is still examining the assessment and/or the information which can be gained when the system created by the PNR Directive is applied to certain EU flights. Whether the risk assessments of other Member States are applicable to Germany will depend on the individual circumstances and will have to be examined in the individual case with attention to the applicable law. In general, however, sharing assessments would be useful in particular when other Member States' risk assessments relate to routes to or from one's own Member State.

- Prerequisites for and limits to sharing data:

According to Germany's Passenger Name Record Act, which implements the PNR Directive, the PIU may participate in joint procedures for systematic cooperation with PIUs of other Member States to prevent and prosecute terrorist offences and serious crime in accordance with the Act. We are examining whether the kind of information-sharing referred to in the question would be possible under the existing law.

In any case, sharing risk assessments/information would also depend on the source of the information on which the assessment is based. Sensitive data from intelligence services or covert investigations are subject to strict rules on sharing with other Member States and on further use.

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

- After initial consideration, the ECJ judgment does not appear to categorically rule out the possibility of such sharing. However, we are still examining this issue.

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

- After a preliminary review, Germany agrees that, according to the ECJ's judgment, a PIU must seek approval from one of the entities referred to in Article 12 (3) (b) of the PNR Directive before checking data transferred from the requesting authority against data stored in the PNR database. However, we are still examining this issue.

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

After an initial review, Germany believes it is not necessary to share lists showing which routes, etc. in which Member States are connected to the PNR system.

Subject to more detailed examination, it is not necessary to check whether the requesting PIU is permitted to process the requested data. Germany is of the opinion that the requesting PIU is obligated to check whether the legal prerequisites for using PNR data are met.

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

- The frequency of review requires further consideration. The ECJ judgment does not specify definite time periods. With regard to the criteria set by the ECJ, the amount of effort required to conduct reviews must also be taken into account.

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?

- Germany believes that it is possible to include additional routes within a review period if the criteria set by the ECJ are met in the individual case. Processing PNR data for the routes concerned appears to be possible as long as information is available which enables a risk assessment to be carried out. This would seem to apply also to routes which are newly opened by air carriers.

1.e. Do all delegations share this understanding?

In Germany's view, if the system established by the PNR Directive is applied to selected intra-EU flights, the ECJ requires that the risk assessment be reviewed at regular intervals. In this context (paragraph 174), the ECJ does not specify how or by whom this review is to be carried out. Nor does it specify how often these reviews are to be carried out. However, the principle of proportionality and the requirement to remain within the limits of what is strictly necessary (see paragraph 175) as well as the right to effective legal redress must be respected.

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?

- We are still considering what other circumstances could in exceptional cases present objective evidence of a risk indicating that certain passengers present a risk that relates to terrorist offences or serious crime.

- In Germany's view, the question whether data already received and stored could be re-evaluated also raises the question as to which legal basis in the PNR Directive could be used to support such re-evaluation without a concrete request.

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

- In Germany's view, requiring an objective link between punishable offences and the carriage of passengers by air raises many complex legal and practical issues. Although the ECJ refers in paragraph 154 to certain offences listed in Annex II to the PNR Directive which, in the court's view, "are, by their very nature, likely to have a direct link with the carriage of passengers by air", this list is not exhaustive. Because of the ECJ's reference to the remarks of the Advocate General, it is necessary to consider whether the offences listed in point 121 of the Advocate General's opinion have this kind of direct link. And because this list is not exhaustive, it is also necessary to examine whether additional offences are, by their very nature, likely to have a direct link with the carriage of passengers by air.

- If an indirect link between a punishable offence and the carriage of passengers by air can only be detected by an individual review, it would be necessary to determine whether the guidelines for conducting reviews could distinguish between the different kinds of searches.

2.c What other observations should be made?

- According to our preliminary assessment, the ECJ's requirements in paragraph 220 have no relation to the ECJ's requirements in paragraph 259 of its judgment.

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?

- Under German law, flights within Germany are not subject to the processing of PNR data. Germany has no comments at this time.

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

- We have not yet come to a final decision on this issue.

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?

- We have not yet come to a final decision on this issue.

GREECE

1. Intra-EU flights

a. Flight selection

1.a.i. It is common knowledge that a high volume of Third-Country Nationals (TCNs) is attempting to enter the European Union's soil, through the Eastern Mediterranean Route, which comes through Greece, since it comprises the EU's external borders. Upon entering Greece, the majority of them wish to travel to other European countries, mainly, by air.

According to the experience that HPiU has gained so far, it is believed that the collection and processing of PNR data collected by the air carriers that operate intra- EU flights, which arrive on or depart from the Hellenic territory, provides with added operational value for both HPiU, as well as the national competent authorities. Intra-EU flights have been selected for many years, by Foreign Terrorist Fighters, as the typical manner for returning to their citizenship countries unnoticed or at least trying to avoid detection by the Law Enforcement Authorities. Moreover, intra-EU flights are being chosen, even today, from many Organized Groups that transfer illegally TCNs (migrants or refugees) from Greece to the Central European Countries. Sometimes, these migrants that are being smuggled illegally, may constitute trafficking victims. THB networks are often involved in migrant smuggling or at least in cooperation with smugglers. In parallel, there have also been cases where radicalized individuals or persons connected to terrorist or violent extremist groups, take advantage of this phenomenon (migrants smuggling) in order to reach their destinations by air travel, letting the LEAs to assume that they are illegal migrants.

Taking the above into consideration, the added value of intra-EU PNR data to HPiU's operational functions is obvious in terms of combating serious crimes and terrorism. Nevertheless, the interpretative approach followed by the judgement is in favor of limitations regarding the collection of PNR data from all intra-EU flights (justification only by a genuine and present or foreseeable terrorist threat for a specific time period in order for a MS to collect the PNR data of all the intra-EU flights).

The decision according to the ruling lies on each MS. Thus, the potential for a fragmented PNR "ecosystem" throughout the European Union is very high, since each MS will be obliged to provide their own (maybe unique) justification. Moreover, failing to do so (providing adequate justification), does not exclude the possibility of a genuine and present, but not currently detected or not foreseeable terrorist threat to a MS, to exist.

From HPiU's perspective, EC should examine the possibility of a necessary legislative proposal to be introduced, in order for this gap, that restricted collection of intra-EU flights PNR data creates, to be covered with uniformity. The practice of MSs justifying a terrorist threat before a court, is not considered by HPiU to be ideal.

1.a.ii. First of all, HPiU does agree that the terrorist threat is not easily quantified and rarely limited to a specific time period.

The described filter presupposes that data for all intra-EU flights will be transferred to each MS's PIU and the selection procedure will be carried out on the PIU's side. According to the HPiU, this approach is very much called for, on the grounds of two main reasons:

- EU policy has always indicated that for the facilitation of air transport and in order to reduce the administrative burdens for air carriers, the reporting formalities required by legal acts of the EU need to remain simplified and harmonized to the greatest extent possible. Hence, MSs placing an additional burden to air carriers, obliging them to proceed to the necessary routes' selection, whenever this would be necessary from the PIUs' operational perspective, might not be the optimal solution.

- Selecting routes and updating this selection, that is sharing subtly the result of MS PIUs risk assessment results, with the industry would only undermine the effectiveness of the PIUs and jeopardize the integrity and confidentiality of the intelligence of the LEAs, that have at hand.

HPiU's opinion is that the proposed filter, **could not be considered appropriate**. Washing all passenger data of all intra-EU flights against some databases that lead to specific actions (watchlists included) and storing only the data of the hits (verified positive matches) would serve well the objective of tracking known terrorists or known criminals that are involved in serious crimes (should it be applied for persons sought for serious crimes as well). Yet, in this way only the one of the two main pillars of a PIU's mission, would be satisfied. The other one being **identifying the unknown terrorists and criminals** by rule-based targeting, **would be omitted.**

HPiU suggests that the MS's-side filter for selecting intra-EU flight routes, **should be based on a multi-criteria risk assessment.**

b. Selecting intra-EU flights - technical, organizational, economic and operative issues

1.b.i. HPiU agrees with all the challenges noted in the document and would like to further emphasize on the **economic issues that arise on the MSs' side**. Filtering incoming data by route and -more importantly- deleting by flight (not by message) is not an automatic built-in capability for most of the PNR systems, to our knowledge. So far, such a capability was not needed. The filter on the MS's-side requires such a capability in its PNR system, which in its turn entails costs for system modifications, the extent of which should be examined thoroughly. EC should take the above into consideration and inform MSs, in any case, whether any funds are to be granted to them, for this purpose.

1.b.ii. HPiU conducts, already in the normal course of its business, since the beginning of its operation, in regular basis security risk analysis, in terms of monitoring terrorism and serious crimes that fall under the provisions of the Law 4579/2018 (transposition of EU Directive 2016/681). This way, HPiU ensures an up-to-date picture of the operational and strategic criminal "status quo" that affects the Hellenic territory. Moreover, this approach gives HPiU the capability to collect, manage and analyse PNR data, ensuring the adoption of all the provided legal principles and requirements, since the necessary business processes are carried out upon specific and tangible results, based on specific, real and present cases linked to terrorist and serious organized crime networks' activity.

If it is for the extent of application to intra-EU flights to be determined, then a multi- criteria recurrent risk assessment should be carried out by MSs' PIUs, similar to the one that HPiU already conducts. **The goal should not be limited application, but application limited to the extent necessary.**

c. Efficiency issues related to fragmentation of data collection

1.c.i. HPiU, in order to fulfill its mission, to manage the huge volume of data, collected during its daily operation and to utilize the qualitative data available, has developed and implements a dynamic and specialized security risk analysis methodology, based on risk analysis models such as the European model Ciram 2.0. (dedicated and detailed analysis has been carried out particularly for the flights operated within the Schengen area). The HPiU's risk analysis model has been implemented by specialized and qualified personnel, with high operational and academic awareness, who possess great experience in the strategic, operational and tactical response to cases of terrorism, smuggling of migrants and minors, trafficking in human beings, as well as dealing with cases involving other types of organized crime activities and European internal security threats.

HPiU proposes the formulation and implementation at European level of **a common security risk analysis model for PNR data collection, management and analysis,** based on the already existing structured analytical procedures of the Hellenic PiU. In this context, **our Unit could take the lead in the formation of an additional working group (or a sub working group)**, where PNR information analysts, will be assigned by Member States' PIUs, with the aim of contributing to the development of a common risk analysis model, always under the EU Council support. It is pointed out that HPiU, deals daily with existing and rather extensive migrants and minor trafficking networks, drug and weapons trafficking cells connected to international organized crime, as well as with terrorist groups with international activity, that directly threaten the internal security of the European Union.

1.c.ii. We are in favor of all MSs sharing the results of their risk assessments, as they may contain intelligence that could be exploited by another MS for the purposes of their future risk assessment regarding the already selected routes or the currently unselected ones.

Information exchange restrictions, should be those imposed, by the already existing and applicable regulatory and legal frameworks, under which information and PNR data are exchanged between MSs and Europol.

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

1.d.i. Upon a duly reasoned request, PIUs should be able to share PNR data and results of processing of those data with other MSs, irrespectively of whether those data are collected by them or not, as per our established procedures.

On top of that, HPiU supports the exchange of information between PIUs, concerning the utilization of operational and strategic intelligence material, with the aim of identifying routes of special interest concerning the topics of terrorism and serious organized crime.

1.d.ii. All the legal provisions and requirements defined by both European and Hellenic legislation, as well as particular provisions, safeguards and business processes enforced by our Agency's (HPiD) Internal Regulation and Hellenic Police IT Security Policy are being strictly implemented by HPiU, along with the European and International law's provisions regarding the protection of human rights, personal data and information. In this light and in full alignment with the above legal requirements, PNR data processing, is carried out without any violation of human rights or data protection principles, only for the purposes of prevention, detection, investigation and prosecution of serious crime and terrorism.

In addition, HPiU already evaluates every incoming PNR request based on the principles of necessity and proportionality, as well as the general rules that derive from the PNR Directive and apply to the procedure of request evaluation. Should the obligation of an independent authority's prior review be inflicted on all MSs' PIUs, account might be necessary to be taken of possible delays in the procedures of request handling, especially of those characterized as urgent and with high priority.

1.d.iii. The selected routes should be at the disposal of all MSs, constantly and seamlessly updated, this being the only way to avoid significant unnecessary administrative burden and cover the gap created by the inherent lack of reciprocity between MS raised by the selection of intra-EU flights. HPiU proposes that the creation of a new platform indicating, **in real time**, the routes for which data are collected and by which PIUs, might be necessary to be examined. In order for every MS's PIU to share the same picture, it would also be useful for such a platform to contain historical information.

In any case, when a MS is confronted with a case that involves another MS's route for which the second MS does not collect data, the first MS should provide the latter with the respective intelligence, to be factored in its risk assessment, **ad hoc**, as this could probably lead to a reviewed selection of the latter MS's intra-EU flights.

1.d.iv. HPiU proposes implementation of its risk analysis procedures framework. As a general rule, HPiU proposes that the risk assessment shall be carried out on a 6- month basis, along with an aggregated report – risk analysis product, serving for situational awareness on an annual basis.

Nevertheless, as per Article 2 (3) of the PNR Directive, a MS may decide to change the selection of intra-EU flights at any time. Operational reasons may arise at any time, indicating the need for **ad hoc risk assessment** and addition of a route or exclusion of a previously selected one.

1.d.v. Operational analyses and risk assessment already performed by the HPiU indicate that our country constitutes a **"hub"** and routes that involve Hellenic airports are selected by many criminal organizations (terrorist networks included). Every single new route should be examined separately and assessed ad hoc, after an initial period of data collection. Possible apparent sharing of features, between a new route and an already selected one, could be an indicator to be taken into account.

Furthermore, the cooperation between the PIUs must be intensified, with the frequent exchange of strategic and operational information, which could form the framework, for future identification of new routes and flights, which are used by terrorist and serious organized crime networks. **This framework would be the basis for the development of a Travel Intelligence Sharing Model between the MSs' PIUs.**

e. Review of selecting intra-EU flights

1.e. HPiU shares this understanding – more flexibility meaning the total of the requirements set out in paragraphs 163-169 (as clearly mentioned in paragraph 174).

2. <u>Retention of PNR data</u>

2.a. Assessment of passengers is carried out once – prior to their scheduled arrival in or departure from the MS. Any verification carried out during the initial 6-month period covers the majority of the cases for establishing the presence of objective evidence of a risk, but other circumstance is well put in this point, for the sake of completeness.

The engagement of a subject in a criminal group might be identified, upon intelligence received by a MS's PIU, nearly before the expiration of the initial 6- months period. This alleged "late" identification does not mean, though, that the subject has not been travelling for the previous 6 months (or more), taking part in criminal activities. In such a circumstance, "searches" could be carried out. These searches, seem not to be restrained by the judgement, so criteria (already crafted or new ones) could be utilized for the purposes of dealing with the particular case, in order to examine whether the data could be retained for the whole 5 years or less (proportionate retention based on the particular case).

2.b. Direct or indirect link should be substantiated on a case-by-case basis. Provision of further practical examples by PIUs may lead to an unnecessary classification, while the judgement's point was to define the broad lines, clarifying to the extent possible its concept.

2.c. The judgment's point of view for not including all the intra-EU flights' PNR data under the scope of the PNR Directive, creates a rather "dangerous" gap, which provides perpetrators with the window of chance to exploit this situation and "hide" from the law enforcement authorities within Europe.

According to the judgement, data should be retained for more than the initial period of 6 months only for persons that a risk relating them to the terrorist offences or serious crimes has been established. Nevertheless, in this way **a security hole is created**, as actions of criminal organizations will not be limited to a 6-month period. For instance, in case of an investigation of a terrorist group that has been moving by air for the last 2 years, only data for their past 6-month movements would be shared with the investigating NCA, so the objectives of the PNR Directive in such cases, seem unable to be met.

At the same time, non-EU countries might have a more powerful arsenal, since they will be allowed to maintain PNR Data for a longer period than the EU Member States, a fact that might jeopardize the effective international cooperation of the LEAs.

Nevertheless, the concept of data being deleted after 6 months, involves technical challenges, too. So far, after 6 months and before the 5-year period, data were automatically retained, unless manually deleted (e.g. upon a data subject's exercise of the right of deletion). Modifying each MS's PNR system in order to delete automatically data, after 6 months, but have a capability of manually retaining them for a configurable time-period, seems to be another economic implication of the judgement, against which EU funding support might be needed.

3. **Flights within the territory of a single Member State**

3.1. HPiU does not apply the PNR Directive to domestic flights.

3.2. As no data are collected by HPiU for domestic flights, the application of the mentioned limitations is not a material issue for our country.

4. **Criteria for selecting risk person**

4.a.+b. HPiU shares the understanding that the rules provided for by the LED apply in such cases, yet it is entirely up to each MS to designate the appropriate tools and practices, since LED transposition may differ between MSs.

Concluding Remarks – Wrap up

Taking into consideration the above and bearing in mind the topics raised by the C- 817/19 Case Judgment, HPiU makes the following remarks:

- Greece, as a European country located at the south-eastern wing of the European Union's border line and constantly facing the threat of the unauthorized and illegal entry of persons involved in terrorism and serious organized crime, through migration smuggling flows, envisages to become one of the leading countries, in the struggle to ensure European internal security, through collecting, processing and disseminating Travel Intelligence.

- HPiU proposes the formation of a specialized Working Group (under a Council structure IXIM or separate) on the management of Travel Intelligence issues (including PNR data) at the European level, including the concerned ruling, but also general issues of the air transport industry and travel intelligence sharing, since a multidimensional approach and expertise (administrative, operational and technical) is necessary for the matter.

The proposed Working Group would be, inter alia, responsible for supporting and guiding the MSs' PIUs, as well as other working groups or sub-groups on Travel Intelligence issues.Particularly, for the issues that have arisen from the concerned judgement, as noted above, HPiU proposes the formulation and implementation at European level of a common security risk analysis. HPiU **could take the lead in the formation of such a working group and a common risk analysis model.**

Our agency's expertise and knowledge could be combined with other MSs' experience in order to develop a swift mutual strategy, **which will thwart any loss of essential Travel Information.**

HUNGARY

1. **Intra-EU flights**

a. Flight selection

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

According to our operational experience, the practical application of the PNR Directive contributes significantly to the security of the European Union and to the effectiveness of the fight against terrorism and organized crime. The application of the PNR Directive to intra-EU flights has operational added value, and it is a very important internal public security measure.

Based on the experience of the HU PIU, the processing of PNR data for intra-EU flights significantly contributes to the internal public security of the EU by allowing the check of the movement of certain high-risk passengers with the aim of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, or to have relevant information regarding passengers who have previously been linked to terrorism or serious crime by a competent authority.

The processing of PNR data is a very important law enforcement instrument when identifying unknown individuals who may be involved in criminal/terrorist activities when travelling within the Schengen area.

If PNR data were not collected to intra-EU flights, these individuals could not have been detected, and consequently the internal public security of the EU would have been significantly undermined.

The procedure set out in paragraphs 169-173 of judgment, according to which the collection of PNR data from all intra-EU flights may only be justified only by a terrorist threat, which is genuine and present or foreseeable on the basis of sufficiently solid grounds is not considered realistic.

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?

The scope of the PNR Directive and the PNR data collected in accordance with the Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

With this in mind, it is justified to use the PNR data not only for terrorism, but also in relation to all the offences included in Annex II of the PNR Directive.

The application of such filter would require the review of the logic of the data processing of the high-risk passengers, and the application of such a filter or similar filters would significantly reduce the efficiency and effectiveness of the PIUs, thereby compromising the internal public security of the EU.

Such a filter would only apply to persons already known to the law enforcement authorities of the Member States and would therefore make it impossible to achieve the objectives of Article 1(2) of the PNR Directive, the prevention, detection and prosecution of terrorist offences and serious crime.

It is important to emphasise that the purpose of the PNR data pre-assessment through automated processing is to identify persons who are unknown to the police services and who may be linked to criminal offences listed in Annex II of the PNR Directive.

b. Selecting intra-EU flights - technical, organizational, economic and operative issues

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

It is important to underline that professional experience has shown that potential offenders often change the mode of transport they use in order to reduce the attention of the competent authorities of the final destination (conspiracy) or assume that the security protocols of airports may differ significantly, so that they use airports considered to be less risky for their travel.

We agree with the PRES's discussion paper that if PNR data collection were to be limited to selected routes or specific airports, this would create a number of technical, organisational, financial and other challenges for the PIUs, which would create significant additional burden on their day-to-day operations.

According to the current design of the HU PIU's PNR system, data are subject to a prior structural and formal check in order to ensure that any sensitive data that may be received from airlines are deleted and are not analysed or stored in any way.

If it is decided that periodic screening is necessary for certain destinations, the appropriate settings in the software would allow the data concerned to be deleted and not analysed or stored. HU supports the idea to implement it on PIUs level without notifying the carriers, meaning that the carriers would not be made aware of the PIU choice and its adjustments.

It should be noted that the removal of PNR data from individual destinations from the system without processing them would require significant development costs and additional administrative tasks for the PIUs.

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

According to the Hungarian practice, it may be necessary in the future to compile a list of countries and airports according to a threat assessment for which the HU PIU continue to maintain data transfers.

This list would be subject to continuous review by the HU PIU on the basis of current indicators (e.g. changes in crime trends, changes in migration-related crime trends, changes in travel patterns, etc.) and its content could be changed accordingly.

This would, in our view, meet the requirement to process PNR data only from specific destinations of intra-EU flights, while allowing the system to react in near real-time to the constantly changing circumstances.

However, it should be noted that this will definitely generate additional workload.

c. Efficiency issues related to fragmentation of data collection

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

In the future, it may be necessary to develop a set of criteria for determining the specific coordinated threat assessment (including, inter alia, the risk index of passengers on a given route, flight density, traffic data, quality of data from a given destination, past experience, law enforcement information) based on a complex assessment of the widest possible range of information.

It is also necessary to develop and implement a system, which gives place to ad hoc and periodic reviews of certain threat assessment.

During this assessment, relevant data deriving from EU trends, reports and the relevant experience and contribution of the PIUs should be taken into account, as well as the expertise of MS's other law enforcement services. The use of existing and future risk assessments done by EU agencies (Frontex, Europol) and other stakeholders can contribute effectively to this assessment, however the contributions of the national law enforcement sector are extremely important.

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?

It is of great importance for effective cooperation if the PIUs to draw up and regularly update the list of destinations identified as risky, based on jointly defined standards.

By sharing risk assessments with other Member States, PIUs can contribute to enhancing the EU's internal public security by supporting each other's activities.

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

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

Yes, we agree with this statement.

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

This would generate a significant amount of additional workload and could slow down operations considerably.

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

The registration of the fact that which PIU in which Member State collects PNR data from which destinations could only be done at national level, which is a good practice, therefore we would agree to maintain it.

Nevertheless, after implementing such an instrument the effective exchange of information between MS could be cumbersome, since the PIUs will not have an up-to-date information on which MS collects PNR data on which flights.

One of the purpose of the PNR Directive is to ensure that all relevant and necessary PNR data or the result of processing those data is exchanged between the PIUs. The aim is that MS can exchange PNR data amongst each other in an effective way, thus reducing the burden on PIUs of both irrelevant and unnecessary requests for information and the impact that it has on the available resources.

Finding the most appropriate solution definitely takes time, and in order to develop the best practices, the experts of the PIU community have to work together in developing and identifying common ideas and concepts that are worth to implement into the daily work.

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

A periodic review system (e.g. 6 months) should be designed, developed and implemented, and the possibility of ad hoc reviews (e.g. in case of changed safety circumstances, operational experience from partner organisations, new flights, etc.) should be created.

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?

Yes, it is justified.

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

The data protection safeguards in the PNR Directive guarantee the necessity and proportionality of collecting and processing PNR data, however it is important to further develop (in line with the judgment), and in particular through legislative review and other soft law instruments the data protection safeguards that clearly demonstrate the proportionality and necessity of the fundamental rights interference during the processing of PNR data. It should be noted that there is agreement that this type of data processing is considered legitimate in terms of its purpose and instruments.

2. Retention of PNR data

The data retention period of PNR data should be kept in five years, because according to our operational experience it is needed to ensure the effective investigation and prosecution of terrorist offences and serious crime listed in Annex II of the PNR Directive.

Since the investigation and prosecution of this offences usually involves several months or sometimes even years, the distinction between initial 6-months retention period and 54-months period is not considered realistic.

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?

The PNR system of the HU PIU is designed in accordance with the provisions of the PNR Directive, the data retention period does not exceed five years.

According to our professional opinion, it is justified to maintain the general practice of retaining passenger data for a period of five years, because practical experience has shown that in many cases passengers have subsequently been found to present a significant risk.

If it is needed in the light of the judgment and its findings, the general retention period may need to be fine-tuned, but this will in any case entail development work and therefore costs.

The reassessment of the already stored PNR data based on new criteria/profiles should not be the basis for the operation of a PIU.

According to our experts, the reassessment of the PNR data could contribute to the identification of specific behavioural patterns and make links between known and unknown persons.

However there is a need to reassess the already received and processed data, which may reveal new travel patterns and characteristics that allow for improved targeting. However, in our view this could only be done by human experts, not an automatism.

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

Through the detailed analysis of the high-risk passengers, on how they travelled, on what route and frequency and analysing their travel history could significantly contribute on targeting, and on the fine-tuning of the profiles.

2.c What other observations should be made?

We are constantly monitoring changes in travel patterns and in the air transport environment, and adjust our profiles and risk analysis methodology accordingly. Incorporating these experiences into our daily activities helps to achieve a higher professional level and improved targeting.

3. Flights within the territory of a single Member State

This is the competence for the Member States concerned to decide, there is currently no such public air traffic in Hungary, therefore this issue is not relevant for us.

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

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

It is necessary, on the one hand, to create and update the internal handbook / manual for operators and analysts on the process of handling high-risk passengers, as well as on how to conduct the analysis and the related workflows.

It is also necessary to make available to data subjects an understandable version of this manual, containing exclusively public information.

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?

This information package for data subjects referred to in answer 4.a. should also include the legal provisions on data processing (PNR Directive, the Criminal Data Protection Directive (LED), national legislation, etc.) as well.

IRELAND

1. **Intra-EU flights**

a. Flight selection

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

For information, Ireland has not legislated heretofore to collect intra-EU PNR data.

The drafting of future legislation to allow Ireland to collect intra-EU PNR data will take the requirements of the ECJ judgment in case 817-19 into account.

Ireland considers that while not impossible and depending on the level of threat that may present at any time in the future, it would be challenging to obtain approval for the future collection of all intra-EU PNR data by a terrorist threat which is genuine and present or foreseeable on the basis of sufficiently solid grounds, as required by the judgment.

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?

Ireland is closely following discussions on operational consequences flowing from the ruling in ECJ case 817-19. Ireland reserves scrutiny on this suggestion, pending legal consultations.

b. Selecting intra-EU flights - technical, organizational, economic and operative issues

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?

Regarding the suggestion that in future, intra-EU carrier data would be transmitted but deleted immediately after reception on an ongoing basis except for routes that are selected for collection, Ireland is of the view that a more workable solution may be to maintain technical connections with intra-EU carriers - so that when a selected route is identified for collection, then the PNR data flow can be "switched on" with minimal technical delay and preferably without prior notice given to the carrier, in order to ensure operational confidentiality.

However, the technical challenge in implementing such a system should not be underestimated, and this approach will be subject to legal advice and agreement at EU level.

c. Efficiency issues related to fragmentation of data collection

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

Ireland supports the proposal made by a number of MS calling for the establishment of an expert working group under a Council structure (IXIM or other) that would be tasked with the development of a non – mandatory risk assessment methodology and the execution of it, in order for the member states to work collaboratively on the motivation of the necessity to collect information for a large majority of intra-EU flights.
The establishment of such a working group would be without prejudice to the right of each Member State to make its own decision on what intra – EU flights would be selected based on its own individual mandate for safeguarding national security, which remains a national Member State competence under the Treaties.

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?

Currently, the IPIU of Ireland does not prepare risk assessments. Any such risk assessment potentially prepared in future would be considered for sharing (on a discretionary basis) with other PIUs on a case by case basis, where deemed necessary and appropriate.

With regard to the idea of a threat assessment the paper proposes two options – an EU level assessment, or for the Member States to be "mutually aware" of the risks assessments elaborated by other Member States.

We would see merit in an EU level assessment if it were clearly for the purpose of the PNR Directive, and therefore limited to terrorist threat. This would prevent any misunderstanding around competence as it would ensure that it would not cloud the issue of national competence regarding national security matters.

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

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

Subject to legal clarification, Ireland is of the view that it continues to be possible for a 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.ii. Do all delegations share this conclusion?

Ireland shares this conclusion.

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

Ireland proposes that PIUs may utilise existing secure networks (for example; the Europol ROVER network) to share up to date and accurate information on the list of selected flights (routes, airports and travel patterns) that each PIU collects PNR data on.

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

Ireland proposes that the selection of intra-EU flights should ideally be reviewed at least every 12 months on an ongoing basis and on an ad hoc basis depending on changing circumstances.

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?

Yes

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

Pending further clarification, Ireland shares this understanding.

2. **Retention of PNR data**

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?

Ireland reserves scrutiny on this question, pending legal consultations.

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

2.c What other observations should be made?

Ireland reserves scrutiny on this question, pending legal consultations.

3. **Flights within the territory of a single Member State**

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?

Under existing legislation, Ireland does not apply the PNR directive to domestic flights. Drafting of future legislation will take the requirements of the ECJ judgment in case 817-19 into account.

4. **Criteria for selecting risk person**

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

With regard to the requirement in the judgment that competent authorities ensure, without necessarily disclosing specifics, that the data subject is able to understand how these criteria and assessment programs work, it would appear that this would need to be resolved at MS level.
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.

This scenario would therefore arise in the context of national judicial proceedings, and as such, requirements would likely be dependent on national criteria around procedural law. In terms of the question raised regarding what mechanisms could be employed to provide required information to data subject while avoiding prejudice to future deployment of criteria, it would seem that a code of practice may be an appropriate means to provide for same which would set out fair procedures and would be developed and agreed at MS level to ensure a consistent approach.

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?

Ireland reserves scrutiny on this question, pending legal consultations.

ITALY

1. ***Intra EU flights.***

   a. ***Flights selection***

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

This is not a realistic scenario. A possible option could be gathering PNR data referred to all operated routes transmitted by air carriers (avoiding to request to the air carriers to filter and limit data transfer), which will be selected and the unnecessary ones will be **immediately deleted**. Based on the results of the threat assessment, only those PNR data of interest to fight against terrorism and serious crimes, will be stored in the PIU dedicated data base and processed only in presence of a "duly reasoned request". The results of PIU analysis will be eventually shared with the competent Authority (others PIU, NCAs or Europol's Operational and Analysis Centre - Travel Intelligence). This option would permit the independent activity of the PIU, aiming at keeping the data confidencial, avoiding to disclose to the air carriers the list of routes of interests. By doing this, the access to PNR data is not applied indiscriminately to all passengers.

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?

By experience, the collection of PNR data and its processing cannot only be referred to terrorism and it **must be applied also to serious crimes**. Terrorists and serious crimes offenders move among the Countries without borders and limits, therefore, it seems to be necessary to underline that PNR is not a massive tool which applies an indiscriminate control. Very difficult to limit the impact of a terrorist threat to one period, to certain routes or travel patterns or even to certain airports, at the discretion of the concerned Member State. Furthermore, filtering PNR to relevant database only to explore the "alerts" could take out of the scope all unknown subjects of interest for leading police investigation teams.

b. Selecting intra-EU flight – technical, organizational, economic and operative issues.

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

The certification procedure of airlines, as a necessary and preparatory step to the sending of PNR data, requires long periods to set it and do not allow the easy selection of intra-EU routes activating or de-activating them only in the event of a specific need or threat. Therefore, in order to mitigate the risk of overcharging the related activities, air carriers will not be required to increase their procedures and the PIU could be responsible for "selecting" concerned routes as a result of a dedicated threat assessment.

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

The most appropriate option is applying the intelligence led principle by keeping only PNR data referred to those flights operated on routes of investigative interest, to be further processed according to established criteria set at domestic level within a EU wide open approach.

c. Efficiency issues related to fragmentation of data collection.

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

In the context of our already consolidate fruitful cooperation, we are in favor of sharing methodology which, may also take into account the multi- modal approach and the necessity for some Countries to collect passengers' data on other modes of transport.

To this regard, we underline Our proposal to seek Europol support to Member States in conducting a tailored European threat assessment and guide domestic interventions.

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 MSs? What would be the prerequisites and limitations of such an approach?

In principle yes, however Member States' National Competent Authorities should be informed and agree on the opportunity to share their own risk assessments with other PIUs within the EU MSs.

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

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

We believe that a Member States' position completely different one from each other will create lacunes and gaps on this matter. The lack of information concerning passengers' data travelling on specific routes on flights operated among Member States, has been so far mitigated through mutual support which is completely different in the event of having the opportunity to collect passengers' data on selected routes whose interest could be different from one to another Country.

A significant innovation introduced by the EU PNR Directive was the overcoming of the concept of risk routes, therefore the hypothesis of a return to this option would represent a leap into the past, in spite of the efforts of Member States to adapt existing systems or create new ones, in order to comply with the PNR Directive's requirements, also taking into account the significant economic damages, deriving from the use of national and European Funds.

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

The PNR data collection and the activities carried out by staff members of the PIU can be regularly reviewed and independently verified by the Data Protection Officer which refers to the national supervisory Authority. Furthermore, in the event of pseudonimized data, the authorization to unmask and make them available is issued by a Leading Judicial Authority or by the Deputy Police Chief, Central Director of the Criminal Police, which provide their authorization according to the principles of necessity and proportionality. That said, the intervention of a domestic independent Authority could be unnecessary.

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

In the event of a return to the identification of risk routes for selected crime areas, the involved PIUs would surely face issues which would be difficult to avoid while selecting routes.

Seeking EU MS consensus on general methodology to be applied to selected routes also via the constitution of an Expert Steering Group set up ad hoc for this activity.

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

In case of a risk assessment concerning the selection of intra-EU flights also based on Europol's support, this could be reviewed on 6 months up to a maximum of one year basis.

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

The selection methodology should have a certain degree of flexibility to quickly adapt to the different challenges / threats we have to face.

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

In principle, in the event of PNR data collection applied to all intra-EU flights, we would support the setting of an independent revision process with the involvement of designated DPO for PNR matters.

*2. **Retention of PNR data.***

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?

By experience, supported by study cases we would stress the importance of collecting passengers' data which may be necessary when they are useful for investigative purpose and the unique tool aiming at identifying an unknown targeted person even if not yet resulting of a positive match.

For instance, suspects, associates and family members of a fugitive may provide him assistance with the aim to escape the sentence, in some cases even by resorting to broken travels in order to avoid being checked and tracked by LEAs.

Having regard of the above, the retention period can not be limited to a very short period and if needed for investigative purpose, it may exceed 6 months.

To this regard we believe that PNR data should be available in clear for 6 months and subsequently should be depersonalized through masking out of all sensitive data element which could serve to identify directly the passenger to whom the PNR data are related to.

The maximum data retention period could be less than 5 years currently allowed by the law, after a period of observation which duration may vary taking into account the assessment carried out by those PIUs that already had to proceed with the cancellation of data. During such period we may monitor and observe the percentage of cases which it was necessary to proceed with the unmasking process and the other cases to be kept.

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

In light of the above, even if not directly involved in a criminal activity the addressed person may be considered as the only link with the targeted subject as better described in attachements 1 to 5.

2.c What other observations should be made?

To this regard, based on real cases we have prepared the attached case studies, related to different crime areas which better illustrate the meaning of words "sufficient ground" and "reasonable suspicion" (attachments 1 to 5).

3. Flights within the territory of a single Member State.

This is not applicable in Italy, in fact the current legislation, allows to gather passengers' PNR data when they are travelling on a flight operated on a national route, only when it is a single element of a trip which also involves intra/extra-EU Countries.

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.

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

In compliance with the current legislation PIU staff members are enabled to check available national, European and international databases, in order to assist them to evolve from a simple piece of information into intelligence and contributing to support leading investigators.

According to provisions of art. 5 of the PNR EU Directive, Member States shall ensure that a data subject has the right to contact the data protection officer (DPO), as a single point of contact, on all issues relating to the processing of that data subject's (PNR data). Such system is already in place and it has been also implemented through the publication on the Department of Public Security's website describing the access procedure for citizens aiming at exercising their own rights. Moreover a list of Frequently Asked Questions were also made available in order to clarify any doubts regarding the use of passengers data record (PNR).

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

The PIU work is regulated by SOPs, in the event of such a specific request, the Data Protection Office is involved, in order to appropriately select which range of information may be disclosed.

Case Study 1

on how the use of PNR data has contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime (THB).

Member State PIU:
ITALY
Date: July / August 2022

PNR data analysis referred to an ongoing german investigation against an Organized Crime Group dealing with Trafficking in Human Beings.

On 25/07/2022, German PIU has requested (Siena ID: 1990730-1-1) PNR data referred to **an email address**, aiming at giving an identity to its user or to those people which may have travelled with bookings realized by using the same contact's details.
Subsequently with the Siena ID: 1993171-1-1 dated 19/08/2022 German PIU has sent a new request **concerning a targeted person**.
The analysis of contact's details revealed the use of **the same email address** which had already emerged as contact detail as better described in the previous Siena case (1990730), *probably linking to a contact person or a travel agency based in Athens*.
Further in-depth assessment conducted on it enabled to collect the reservation's details related to a new PNR code referred to a broken travel **in relation to the same person**.

Further analysis conducted on the aforementioned contact details, also allowed to gather information related to **several** reservations which were referred to "***one way***" trips and the related passengers (with a ***specific range of age***). All of them are supposed to have **citizenship different from the Greek one**, therefore the recourse to a travel agency based in Athens appears quite peculiar.

Case Study 2

on how the use of PNR data has contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime (murder).

Member State PIU:
ITALY
Date: August 2022

PNR data analysis referred to an ongoing Czeck investigation in relation to a case of murder.
On 27/08/2022, the Czeck Republic PIU has requested (Siena ID: *2014239*-1-1) PNR data referred to targeted person, suspected to be involved in a murder. The requested person has been tracked in our PNR DB which has collected the information referred to a PNR code linking to him and a co-traveller, probably unknown to the requesting PIU. The analysis of contact's details revealed the use of an email address and a phone number both linking to a Company based in Prague. The sponsor for the related payment (better described in the Form Of Payment field) also appeared as contact person of the aforementioned Company. The PNR data analysis conducted on the co-traveler has also revealed information related to 2 different reservations, the first referred to the known targeted person, while the second reservation was referred to the still unknown person. According to the details concerning the travel itinerary, both subjects would have travelled in different dates, from Bologna (BLQ) to Munich (MUC) and subsequently from Munich (MUC) to Prague (PRG). The RCI (Reservation Control Information) and IFT (Interactive Free Text) fields revealed that both reservations had been realized by the same IP address, providing the same contact details (phone number and email address), referred to the unknown person.

Case Study 3

on how the use of PNR data has contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime (Drug Trafficking).

Member State PIU:
ITALY
Date: January 2021 / September 2022

PNR data analysis referred to an ongoing NCAs investigation in relation to a case of Drug Trafficking and the search of a High Value Target.

Since the beginning of 2021, the Italian PIU is supporting the Carabinieri Corps - Investigation Unit of Naples which are dealing with a complex investigation aimed at locating a fugitive member of a Camorra-style criminal organization hit in 2013 by the Arrest Order from the A.G. of Catania having to atone for 20 years of imprisonment for international drug trafficking.

Based on available information the PIU has started a profiling activity on PNR data relating to the associates and family members provided by leading investigators in order to track their movements (involving France, The Netherland and Spain). In particular taking into account the duly reasoned request details (the former partner and their daughter currently live in Spain), to receive information on the movements of suspects as a result of watchlisting activity. The analysis of PNR data provided by the Dutch and French PIU, permitted to track a reservation referred to the fugitive's former partner and their daughter, which had travelled on a Paris Charles de Gaulle - Dubai flight and back (probably trying to avoid the check of spanish Authorities).

The analysis also highlighted the presence of a suspect still unknown to the Competent Authorities, this latter in fact had previously travelled from Panama to Paris and subsequently from Paris to Dubai along with the fugitive's partner.

In conclusion, the new elements were immediately transmitted to the aforementioned Competent Authority, highligting the Panama / France / Dubai connections and the possible implications on the location of the fugitive and the criminal activity that he could carry out.

Case Study 4

on how the use of PNR data and the watchlisting activity has contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime (drug trafficking)

Member State PIU:
ITALY
Date: June 2022

Investigation aiming to locate a fugitive

The PIU has supported the State Police Organized Crime Squad of Lecce (one of our National Competent Authorities), which have carried out complex investigations led by the competent Public Prosecutor, against the targeted subjects members of an organized crime group, dealing with drug trafficking conduct at international level. OSINT and data enrichment activities on the targeted person revealed that she should have lived in Benalmádena (Malaga). Based on available information, supported by technical activities, namely ongoing wire tapping the targeted person would have travelled among European Countries, in particular to/from Spain in order to reach an unknown final destination where probably meeting her partner, which is a fugitive, searched at international level, with a leading role in the OCG.
The watchlist on the targeted person allowed to trace her travelling on a Ryanair flight from Ciampino (Rome) to Malaga (Spain) with the minor daughter.
On 14/06/2022, the Italian fugitive, partner of the targeted person, which the watchlist was referred to, has been arrested in Malaga (Spain).

LA GAZZETTA DEL MEZZOGIORNO

L. CASO

Lecce, arrestato in Spagna uno dei 100 latitanti più pericolosi d'Italia

La cattura è giunta al termine di una complessa attività d'indagine, coordinata dalla Direzione Distrettuale Antimafia della Procura della Repubblica di Lecce

14 Giugno 2022

Redazione online

Case Study 5

on how the use of PNR data and the watchlisting activity has contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime (money laundering and fraudulent activities).

Member State PIU:
ITALY
Date: April 2022

Investigation aiming to locate a fugitive

The Italian PIU has supported the State Police of Cagliari (one of our National Competent Authorities), which have carried out complex investigations led by the competent Public Prosecutor, against the targeted subjects members of an organized crime group, dealing with money laundering and fraud at international level. The OCG members with deep knowledge of the international financial world allows the associates of such criminal group, with an enormous monetary depth and with currency flows for many millions of euros and other currencies, taking advantage of different Modus Operandi. The manager of an Italian company, supposed to be the main target with a leading role within the OCG, was not available in Italy. According to the leading investigators he had probably moved to Serbia which was also confirmed by the analysis of the spending of his credit card. Based on available information, his brother and his sister also under investigation on 16/03/2022 had left Cagliari (Italy) probably to join him somewhere in a still unknown location. Intelligence gathered suggest that the OCG members have been traveling among the European countries, in particular to/from Hungary and Romania during the requested period, with the aim to reach Serbia and Switzerland where they manage their illegal business.

On 20/04/2022, as a result of a joint (IT-HU-RO PIUs) watchlisting activities the Italian searched person has been arrested at his arrival at the airport of Cagliari.

ANSA.it › Sardegna › Maxi truffa da 4,5 mln, due arresti nel Cagliaritano

Maxi truffa da 4,5 mln, due arresti nel Cagliaritano

Dall'inchiesta emergerebbero migliaia di vittime

Redazione ANSA
CAGLIARI
20 aprile 2022
10:07
NEWS

Suggerisci
Facebook
Twitter
Altri

Stampa

Scrivi alla redazione

di Manuel Scordo

I clienti da truffare venivano agganciati in occasione di convention e feste in cui spiccavano invitati vip e personaggi dello spettacolo.

Eventi di lusso, uno anche a Dubai, che in realtà erano solo uno specchietto per le allodole per tranquillizzare i possibili clienti e convincerli ad affidare loro ingenti somme di denaro da investire, promettendo facili guadagni.

LATVIA

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

In LV, the collection of PNR data from all intra-EU flights based solely on a high terrorism threat level is currently not a realistic scenario. The opportunities to substantiate a non-selective data collection with other significant (equivalent) threats to national security are evaluated.

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?

LV believes that the use of pre-defined criteria can be useful, however it cannot help to achieve all objectives of the PNR Directive[1] (investigation and prosecution of terrorist offenses and serious crimes). Achieving these goals often requires data on persons who have not previously come to the attention of competent authorities and thus are not included in the checklists/filters.

In this regard, LV would invite to discuss the possibility of introducing alternative (compensatory) data protection mechanisms that would allow continued data collection/storage within the current scope, respecting the requirements of the Court of Justice of the EU (hereinafter – CJEU). For example, complete masking or even encryption of intra-EU flight data immediately after receiving them. Unmasking of those data would be possible only with a special permission of a competent third party (e.g. a judge or other authorized person). A similar mechanism would also apply to data older than 6 months (see section 2 – Retention of PNR data).

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

It would be highly beneficial to consider data transfer separately from data processing. Otherwise, it is likely that air carriers will not be able to adapt to the changes in the given selection of intra-EU flights from which PNR data has to be sent. It will also create communication and cooperation challenges with the industry representatives.

---

[1] **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).

Thus, if the LV suggestion regarding the introduction of alternative (compensatory) data protection mechanisms (please see LV reply to the previous question) could not be implemented, LV believes that it would be more useful and secure to receive PNR data on all intra-EU flights and then to mask/encrypt/delete them depending on the operational scenario and risk situation adopted by the PIU.

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

If the LV suggestion regarding the introduction of alternative (compensatory) data protection mechanisms could not be implemented, in order to minimise the operational impact of the CJEU judgement in case C-817/19 (hereinafter – CJEU judgment), LV proposes masking/encrypting the PNR data of individual intra-EU flights depending on the operational scenario and risk situation adopted by the PIU. Unmasking of those data would be possible only with a special permission of a competent third party (e.g. a judge or other authorized person).

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

In LV view, the EU-level criteria for the route selection could be beneficial. However, it must also be borne in mind that each Member State also has its own unique risk factors that could influence risk route selection. In any case, route risk analysis must be performed using both analysis of historical data of this route (e.g. the number of previously identified risk passengers) and current forecasts and criminal intelligence information.

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?

In practice, such sharing of risk assessments with other PIUs could be possible, but to a limited extent. Some threats are unique to certain Member States or regions. In addition, some threats may be related to very sensitive information (including in the field of national security). The state of play regarding the development of common PNR risk profiles clearly demonstrates the limited capabilities and willingness of Member States to share sensitive risk information.

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

In LV view, the CJEU judgment does not limit the current practice of data exchange between Member States.

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

LV agrees with the PRES assessment.

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

Most likely, a new technical instrument at EU level would be needed, for example, a secure and interactive automated platform for the exchange of such data between Member States. However, it would be difficult to implement it in practice.

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

It should be reviewed as often as necessary based on operational needs.

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?

Yes, depending on the initial risk criteria.

1.e. Do all delegations share this understanding?

LV agrees with the PRES assessment.

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?

The main argument for storing PNR data of longer than six months is not directly related to the initial risk assessment. The practice shows that historical data (>6 months) are more useful as evidence in investigative and judicial processes that take much longer time. In order to achieve the objectives of the PNR Directive (investigation and prosecution of terrorist offenses and serious crimes), historical data on persons who have not previously come to the attention of the competent authorities and thus are not included in the checklists/filters are often required.

In this regard, LV calls for evaluating the possibility of introducing some form of special masking/encryption mechanisms which would allow Member States to maintain some form of strictly limited and controlled access to all historical data (<5 years).

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

Direct or indirect objective link should be determined on a case-by-case basis.

2.c What other observations should be made?

In accordance with LV preliminary interpretation, the criteria mentioned in the CJEU judgment are consistent with the current practices of Member States' PIUs in relation to risk assessments – the use of external risk information, direct matches against watchlists and information systems or possible matches based on risk rules. Accordingly, the CJEU allows the storage of PNR data of all passengers for whom PIU has previously obtained any type of hit or other risk information or whose data is still required for such assessments in the future.

3.1 What is the position of delegations?

LV considers that domestic flights are out of scope of the CJEU judgment.

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

No.

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

The established approach in the context of Article 15(1) of Directive (EU) 2016/680[2] should apply.

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?

The maximum generalization of criteria, for example, referring only to the categories of criteria used (for example, booking information, document information etc.).

Other remarks by LV

Considering the significant operational impact of the CJEU judgment on the EU PIU community, LV highly appreciates efforts undertaken by the PRES in order to raise awareness and promote dialogue on this topic. Continued support by the EU Council is highly encouraging to the MS when dealing with legal uncertainties.

LV believes that a coordinated EU-level approach to this difficult issue is the only way to maintain an effective EU PIU network and significantly limit negative operational impact of the judgment. LV strongly supports continued efforts by all involved parties to elaborate joint and concrete EU-level solutions to the most problematic aspects of the CJEU judgement with the utmost urgency.

LV also supports and encourages any activities undertaken by PRES, COM and other MS aimed at finding a sustainable long-term solution for the challenges presented by the CJEU judgment, including, but not limited to new EU-level legislative initiatives.

[2] **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 (EU OJ L 119, 4.5.2016, p. 89).

LITHUANIA

The implementation of the main provisions of the court decision related to the collection of Intra-EU flights and the period of PNR data storage will have a negative impact on the effectiveness of the processing and use of PNR data.

We call on the European Commission as soon as possible to submit a new legislative proposal on the processing of passenger data in the EU, which would establish the clear, comprehensive, efficient and sustainable collection and processing of passenger data (API and PNR) for the purpose of combating serious crime and terrorism. At the same time, it would adequately address the concerns outlined in the ruling of the Court of Justice regarding possible risks in the protection of personal data.

1. Intra-EU flights

- ✓ It would be difficult for Lithuania to genuinely set a heightened terrorism threat level over the long term. In light of that, we would not be able to collect all PNR data on this basis on a regular basis.

- ✓ Cooperation with air carriers should not be changed. Air carriers should provide all the data and it should be filtered before entering the system. Only the passenger data of the destinations that have been identified in the risk assessment by the national authorities should be entered into the database (PNR IS).

- ✓ Europol should take the lead in EU-wide risk assessment and this assessment should be the basis for MS national risk assessments, but MS should have the right to decide as they best know their internal situation. Accordingly, the MS risk assessment cycle (periodicity) must be linked to the periodicity of Europol's analytical products.

- ✓ MS should share data regarding identified flight directions. This information should be available on EPE ROVER as well.

2. Retention of PNR data

All PNR data collected should be retained for a minimum of 6 months. In the cases, provided below, data should be retained for up to 5 years:

- persons matching (hits) with risk assessment;

- persons for whom the PIU received duly-reason requests from competent authorities;

- risk assessment justifies the collection of passenger data for the relevant flight.

3. Flights within the territory of a single Member State

Due to the size of the country, Lithuania has no domestic flights and so the PIU of Lithuania does not collect such data, thus this issue is not relevant for Lithuania. In addition, the court does not unequivocally speak on this issue, we believe that states should be able to decide independently on the processing of such data.

4. Criteria for selecting risk persons

Disclosure of such information poses a threat to the operational efficiency and risks disclosure of operational tactics. Only very general information about passenger data processing criteria could be made public. Although procedures for assessing such information can be provided in a classified manner, this could still result in the unwanted disclosure of the criteria if the court examining the complaint is provided with more specific information about the criteria and the functioning of the profiling mechanism. This would lead to the ineffectiveness of such criteria.

NETHERLANDS

General remarks:

NL would like to express appreciation for the efforts undertaken by the Presidency to promote discussion on the judgment of the Court on PNR. A coordinated EU-level response to the judgment can ensure the ability of Member States to uphold a strong framework for the use of passenger data in the fight against terrorism and serious crime, while at the same time ensuring a continuous high standard of data protection.

NL welcomes any initiatives by the Presidency, Commission, and other Member States addressing the challenges presented by the Court's judgment, including but not limited to (new) EU-level legislative proposals.

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

NL encourages a discussion on procedures for the selection of flights to be used when the threat level does not necessitate the collection of PNR data of all intra-EU flights.

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?

NL would appreciate clarification on how this procedure relates to the issue of data processing vs. data transfer as discussed on pages 4 and 5 of document 11911/22. Furthermore, NL would like to call attention to the importance of requests for historical data made by competent authorities for the goals of the PNR Directive.

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

It is essential to continue to ensure a high level of data protection. To this end, a broad consideration is needed that includes the data protection risks resulting from selecting certain intra-EU flights. This includes the risk of unlawful processing as a result of errors in data transfer, as well as the risks to privacy and security resulting from sharing information requests and operationally sensitive flight selections with private parties.

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

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

NL is open to discussion of EU-level criteria to be used for the selection of flights. Besides EU-level risk criteria, however, the circumstances and risk factors of individual Member States may differ. Discussions should also include the level of analysis, which can vary from individual flights to airports.

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?

Sharing risk assessments is possible at a generalized level. The information to be shared should not include any personal data or information that could serve to identify passengers directly. Furthermore, caution should be exercised in sharing information specifically applicable to a certain route or airport.

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

While we do acknowledge the flexibility the court judgment provides in applying the directive to intra-EU flights including the sharing of information between PIUs, we would appreciate further elaboration on the possibilities for extending the scope of information to be shared.

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

The Netherlands supports this conclusion.

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

This issue likely requires an EU-level technical solution through which Member States can exchange information while maintaining the appropriate level of data protection.

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

This will depend on the manner of limiting the application of the Directive to intra-EU flights. However, the chosen solution should take into account the operations of the aviation industry and minimize the sensitivity to mistaken and unlawful processing, while reflecting current operational needs.

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?

Depending on the chosen method of selection and the chosen review period, new flights could be added to the selection.

1.e. Do all delegations share this understanding?

The Netherlands supports this conclusion.

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?

- NL acknowledges the importance of historical data in both ongoing and new investigations. This may give need to an adjustment of criteria as new modi operandi come to light.
- NL would appreciate further clarification on the way this would relate to the current article 6.3(b) of the directive, which refers back to the advance assessment of passengers.
- As an additional circumstance, on a case by case basis, a connection to a known suspect (e.g. a passenger who matches with a request by a competent authority travels together with someone) can be reason to retain a passenger's PNR data.

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

No other examples available at this moment.

2.c What other observations should be made?

No other observations at this moment.

3.1 What is the position of delegations?

The Netherlands has no domestic flights.

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

See above.

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

Art. 15(1) of Directive EU(2016/681) should be applied. Information provided can include general procedural information about the way pre-determined criteria are established.

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?

In order to prevent a negative impact on the future use of pre-determined criteria, information should be generalized where possible, e.g. sharing *categories* of data used in the criteria.

PORTUGAL

1. Intra-EU flights

In Portugal, the PIU workload involving intra-EU flights represents more than 50% of the PNR data. Thus, due to their volume, the lack of these data would have serious repercussions on the PIU's workload and, above all, on the operational results related to combating terrorism and serious crime.

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

Considering the current threat level, PT would not be able to use its terrorist threat to fully justify the PNR data collection on all intra-EU flights.

A solution based on the level of terrorist threat in each MS, variable and sometimes unpredictable, is difficult to implement, and may compromise the overall functioning of PIUs in the EU. Furthermore, the evaluation of terrorism risk should take into consideration the instrumental crimes able to finance terrorist activities, such as money laundering, drug trafficking, arms trafficking, etc. Terrorist offences cannot be analysed by neglecting everything upstream, namely the financial and logistical aspects.

A more consistent and horizontal approach from MS should be a premise and an opportunity for a PNR Directive revision. Moreover, this issue will be probably solved with a PNR Directive revision and the consequent common approach only.

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?

A filter at the member state level to compare PNR data with all intra-EU flights, by means of an automatic process with relevant databases (alerts) could be a good solution, especially if such filter would be applied to serious crime as well, which seems to be possible. This solution reduces the impact of the court decision and allows a minimum level of functionality. Moreover, it does not compromise the effectiveness of the data processing, as criminals do not know which routes are under control, unlike what would inevitably happen if PNR data collection took place on selected routes only. The approach to serious crime has been a pacific criteria and a useful lens for intelligence, and a strong tool to keep up with organised crime plasticity as well. Thus, we should be focused on serious crime as well, instead of focusing on terrorism only. Combating terrorism is impossible by ignoring other instrumental crimes. This may be a better solution for carriers, as it simplifies the push process, such as sending data on selected routes only which requires constant changes, workload, and would be costly.

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

Limiting the collection of PNR data through the action of PIUs, even under the supervision of other authority, rather than limiting the transfer of PNR data by air carriers only, seems an interesting option. In addition, reinforcing audit and compliance, human resources selection and an effective management case by case, can strongly shield the necessary overall security.

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

One option would be masking immediately after the push every personal and privacy data on intra-EU flights, with the exception of data regarding dates, itineraries, etc. The unmasking would only happen in the event of a concrete threat or through a duly motivated request.

By masking the data, it is possible to defend the "transfer" as the data is protected. The "processing" would only take place in justified cases.

Questions?

Will it be possible to apply the control to non-EU citizens on intra-EU flights?

Are the passenger data on intra-EU flights connected to non-EU flights covered by the Court's ruling?

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

The data collection on selected routes only will reduce operational efficiency, as criminals will eventually be able to anticipate routes under control and, therefore, avoid them, emptying any risk analysis attempt and rendering measures ineffective. However, at the same time, this measure is discriminatory.

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?

This issue has not yet been sufficiently clarified, and there is a lack of elements for the adequate analysis.

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

In a first approach, we share this conclusion.

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

Based on what is known so far, in a first approach, we share this conclusion.

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

This issue has not yet been sufficiently clarified, and there is a lack of elements for the adequate analysis.

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

This issue has not yet been sufficiently clarified. Six months seems to be the most appropriate timeframe to coincide with the retention/unmasking deadlines and, simultaneously, with the IATA summer and winter seasons.

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?

Yes, it does seems logical from an operational point of view, and is legally admissible.

1.e. Do all delegations share this understanding?

In a first approach, we share this conclusion.

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?

Yes, it seems logical from an operational point of view, and is legally admissible.

Once again, it is important to emphasise the conceptual difference between "transfer" and "processing".

Assuming that the transfer is admissible for all intra-EU flights, by implementing a mandatory process to mask all personal and privacy data on intra-EU flights, we can evoke the additional protection applied by masking these data to justify a longer retention period.

This issue reinforces the role of the non-personal data. The itinerary, the time of flight, the days between booking and travel, the means of payment, among others, are not nominal (personal/privacy) data and could be used for risk analysis.

By receiving the data from intra-EU flights, masking out all personal data and using the non-personal data, the risk analysis would be possible. Afterwards, in justified cases, unmasking would be requested to a data protection or judicial authority, if necessary.

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

In this regard, and bearing in mind that PNR data relate to bookings, they actually correspond to intentions to travel. In the light of the concept of 'preparatory acts', it may be understood that the mere intention of making a reservation with unusual patterns, with the aim of evading controls, to a particular destination with the purpose of committing a terrorist act or a serious crime is, in abstract terms, sufficient reason to be considered as an indirect link. Examples of this include making a reservation three days before travelling or making several reservations at the same time with the purpose of evading controls.

2.c What other observations should be made?

A balance between a security system, data protection and a safe society is needed. Data accessibility does not imply it is effectively accessed. It should be duly preserved but accessible, upon justified request.

3.1 What is the position of delegations?

Portuguese law does not apply to domestic flights.

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

Portuguese law does not apply to domestic flights.

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

Risk assessment criteria should be based on non-personal elements, itineraries, dates, etc., as much as possible. Thus, this issue is no longer directly related to personal or private data and becomes less relevant. For the most, risk analysis is based on indicators, educating future risk routes and passengers. This analysis is sensitive, but strongly settled on previous experience (for instance, crime statistics, which is, naturally, anonymous).

On specific cases, in order to ensure the exercise of the right to judicial redress against the possible unlawful nature of criteria, information should be provided in collaboration with data protection authorities, or judicial authorities in criminal cases.

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?

The information given to the public concerning the risk assessment criteria should be generic; otherwise, it undermines the effectiveness of the risk assessment.

ROMANIA

The topic in question is being analysed at national level, with the involvement of specialists in the field of personal data protection, legal and information-operational from the competent authorities, therefore the comments reflect the opinion expressed, at this stage, at the level of the RO-PIU and of the beneficiaries of PNR data.

Please note that the comments can be shared with the other delegations of the MS

We appreciate that the data which air carriers are obliged to transfer to the RO-PIU under the PNR Directive are relevant, adequate and not excessive in relation to the purposes of the Directive and do not go beyond what is strictly necessary to achieve those purposes.

The generalised and undifferentiated nature of the transfer of PNR data and the prior assessment of air passengers by means of automated processing of such data is compatible with Articles 7 and 8 of the Charter, which enshrine fundamental rights, respect for privacy, in particular as long as supervision by the National Supervisory Authority for Personal Data Processing is ensured, by means of investigations, inspections and audits, as well as the handling of complaints from any interested person.

Also, according to Article 2 of the PNR Directive, the decision to apply it to intra-EU flights lies solely with the Member States, with the obligation to notify the Commission. Thus, Member States have the right to decide on the extent of the period of time for which they apply the Directive also to intra-EU flights, with the possibility of revoking the written notification to the Commission at any time, without specifically imposing limitations on the number of flights or selecting flights/travel routes. Please note that Romania has decided to apply the PNR Directive to intra-EU flights and has notified the Commission accordingly.

Nevertheless, the CJEU considers that the undifferentiated application of the system established by the PNR Directive to all intra-EU flights is strictly linked to the existence of an actual or foreseeable terrorist threat.

In this regard, we consider that, in the current context of the Russian-Ukrainian military conflict, which has generated massive waves of refugees migrating to the European area using intra-EU flights, threats to national security are real, present and foreseeable.

Moreover, regarding the persons suspected of connections with the terrorist phenomenon, we emphasize the fact that they continue their activity even after entering the European area, and it is necessary to implement/use all the available instruments, without introducing excessive conditionalities, which would limit the capacity of the competent national authorities in the effort to document the cases under investigation.

In this context, PNR data contribute to confirming/completing information on the links of some suspects on the counter-terrorism profile with other persons/extended family group, possible destination/transit states, time spent in certain states/overlap and/or flight routes with other persons of potential interest.

Thus, PNR data from intra-EU flights represent an important law enforcement tool for tracking the movements of known suspects and identifying suspicious travel patterns of unknown persons who may be involved in criminal/terrorist activities. Selective collection, limited to certain flights or timeframes, would affect the process of verifying information on possible terrorist/homeland security threats, the end result could lead, in many cases, to the measure being unenforceable and ineffective.

Concerning the retention period of PNR data, we consider that the data should be stored as long as necessary for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime. Due to the activities carried out by the authorities and the purposes for which they are used, they should be kept for a sufficiently long period of time for analysis and use in investigations, as the proposed period of 6 months is far too limited in relation to them.

For instance, in the case of the investigation and prosecution of terrorist offences, activities which by their nature can only take place after the offence has been committed, the competent prosecuting authorities will no longer be able to request PNR data on a person who has committed a terrorist offence after the initial six-month retention period has expired, but the intention of the legislator was precisely to ensure the possibility of requesting them in such particular cases even after the expiry of the six-month period, as these data constitute an important element of evidence.

In order to ensure a high level of security, the legislative authority has laid down rules in the PNR Directive so that access to the full PNR data, which allows direct identification of the individual, is granted under strict and limited conditions. Moreover, the specific activity is monitored at national level by the National Supervisory Authority for Personal Data Processing in order to guarantee the integrity and security of data processing and the rights of data subjects are also respected.

In the light of the above, we support the idea of collecting all PNR data from air carriers and storing them in the PNR System for a period of 5 years, but processing them selectively, based on specific risk assessments developed at competent authorities' level, in relation to the crime category.

Given that criminal networks are constantly adapting their modus operandi and expanding their spheres of influence in different European countries, exploiting the differences between their legal systems, we consider the need to carry out risk assessments every six months or in accordance with the operational circumstances.

SLOVAKIA

1. **Intra-EU flights**

a. Flight selection

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

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?

The Slovak Passenger Information Unit wishes to express the following:

The PNR data from the intra Schengen flights is currently being checked against relevant databases (SIS2, SLTD, etc.) and as far as the filters are concerned, they would not identify the unknown risk at the time of processing the data. It would also increase the workload of the PIU and the relevant authorities by having to check every "flagged person". At the same time the quality of the PNR data is not sufficient – it only offers first names and surnames.

b. Selecting intra-EU flights - technical, organizational, economic and operative issues

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

Connecting new air carriers into the PNR system is time and resource consuming, in many cases it takes months. Flight routes change frequently and the Slovak PIU could not connect each air carrier in the desired time window to efficiently collect the PNR data**.**

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

It would be helpful to consider risk analyses for every destination country or region as well as a regular evaluation of said risk analyses. In the Slovak republic the flight routes differ every 6 months.

Also PIUs should apply safeguards for transferring PNR data or limit direct access to PNR data from the relevant authorities.

c. Efficiency issues related to fragmentation of data collection

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

The Slovak PIU feels the presented measures are sufficient.

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?

Yes, however we would propose that the access is restricted within the EU for PIUs and for the relevant authorities.

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

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

Yes.

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

No, because in many operational cases the need for rapid response is necessary, therefore any delay in the provision of data could have negative consequences.

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

It would be beneficial to share the selected flights or routes or regions – with EU restricted access for the PIUs.

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

We would propose that they are reviewed every 6 months and ad-hoc depending on the threat assessment, because creating such a report is time consuming.

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?

Yes and furthermore, it is also our opinion that within the threat analyses whole regions should also be considered.

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

Yes.

2. Retention of PNR data

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?

The directive provides all circumstances. The perceived point of data retention is that terrorism and serious crimes are being planned over a long period of time. Whether it is smuggling, or terrorism. These crimes often take a long time to plan, sometime even more than 3 years. There was an instance to even make the data retention longer Therefore, many links are revealed after the first initial information is acquired and historical searches also help to expose unknown suspects. Also threat assessments is based on past information, which indicates that our scope should be longer 6 months.

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

Some examples of these are the usage of the same emails, telephone numbers, credit cards, multiple persons on one reservation trying to pass themselves as one person, booking for different persons and the link to a previous object (email, phone, CC). As well as, rule based targeting resulting from threat assessments.

2.c What other observations should be made?

3. Flights within the territory of a single Member State

3.1 What is the position of delegations?

N/A

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

N/A

4. **Criteria for selecting risk person**

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

Revealing any criteria could possibly jeopardize functional risk assessment.

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?

Revealing any criteria could possibly jeopardize functional risk assessment.

SLOVENIA

1. **Intra-EU flights**

a. Flight selection

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

We agree with the opinion, deriving from the discussion between the Member States, that great majority of the aviation and subsequent processed data on passengers are represented by internal flights. Upon that, we have to emphasize that the terrorism threat assessment among the Member States, which is low for most countries, can differ greatly. Potential perpetrators will always find a way to travel between Member States and they will seek opportunities where the terrorism threat level is low and the operation of the security authorities is adjusted to it. In this manner, a Member State with severe terrorism threat could gather and process this kind of information and another, where the threat level is low, could not. This would lead to great discrepancies and lack of information when we will need it the most. We believe this requires a coordinated approach of all Member States.

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?

We partially support the a/m solution of the so-called filters. However, as a small country with low number of flights in comparison to large Member States and low terrorism threat level, Slovenia could hardly take part in it. On the other hand, we have to take into consideration that we are a part of the EU airspace and that we can successfully gather and process PNR data for the purposes of prevention and investigation of the criminal offence of Terrorism in broader context of the safety of the complete EU only as a whole. With the so-called filters, we also have to consider high flexibility of the perpetrators, who will change their way of travelling and destinations (for example, Member States with multiple airports will face redirection of destinations, etc.). The applicable PNR directive is not restricted to the area of terrorism, it also covers the area of serious criminal offences, since many of them are directly or indirectly related to the area of terrorism (for example Forging Documents, criminal offences related to weapons, criminal offence of Money Laundering,…). The fact is that by detecting these criminal offences, which can be predicate offences, related to terrorism, we can detect the latter. The implementation of filters would also limit us to search/monitoring of previously determined persons. Upon that, we would lose the possibility to search connected persons and search according to the history of travelling for both newly monitored person, as well as the persons, connected to them. We support the solution of unification and coordination of the threat assessment, where the key role could be played by either EUROPOL or EC with Member States.

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

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?

The selection of flights must be based on the threat assessment. The proposal that the Member States would share its list of risk flights with airlines could cause security risks. This is unacceptable.

c. Efficiency issues related to fragmentation of data collection

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?

The exchange between Member States is crucial. The exchange between Member States must be clearly defined and standards have to be set, which must be monitored and supplemented, if deemed necessary. A unified approach on the EU level is necessary. The national legislation of our country allows exchange of PNR data and analyses with other EU Member States and Europol.

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

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

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

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

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

1.e. Do all delegations share this understanding?

2. Retention of PNR data

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?

With regard to the retention of data after the period of 6 months, we agree with the opinion that longer data retention period for the purposes of criminal proceedings is necessary. Upon that, we have to take into consideration that each Member State has set the conditions for access in their national legislation. In most Member States, also in Slovenia, such permit for revealing this kind of information was transferred to judicial authorities, which we support.

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

2.c What other observations should be made?

3. Flights within the territory of a single Member State

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?

Slovenia does not have any domestic flights.

4. Criteria for selecting risk person

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

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?

SPAIN

1. **Intra-EU flights**

a. Flight selection

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

The Spanish delegation would not be able to deal with this situation insofar as it would not be technically possible, since it is very difficult to carry out such a selection of flights by selecting a series of routes because the IT Systems does not allow it and it is very difficult for the police to calculate the exact route that could be used by terrorists.

To comply with the Court's requirements, the only option would be to systematize the alert level to the maximum or, in case of a negative result, to immediately delete all flights after processing.

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

Of course, we may apply this filter such OC as Terrorism, there is not any reminder or reference in the Directive saying that OC is less than terrorism, without mentioning all the links between OC and Terrorism.

Spain consider that establish a seek for terrorism and OC groups and people as a beginning is a very good start, nonetheless considering that any negative result may be deleted from the system in order to comply with the court. Notwithstanding this could give us a disadvantage in the analysis of data in a long term. But leaving the scope of possibilities of PNR data only in reaching results through matching again national or international database leave us without the possibility of detecting "alerts" of unknown subjects.

Anyway, we prefer this choice of losing the perspective but keeping the intra-EU flights.

b. Selecting intra-EU flight – technical, organizational, economic and operative issues

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

Technical and organizational problems have been discussed during several meetings and if in case of deciding who has that responsibility, has to be the PIU in order to mitigate any overload of work in the different air carriers and provide the capacity to the PIU (as has to be) to define and control the patterns of the different searches.

If we assume that we can select threats (that in this case the Spanish PIU could not) and access a series of airlines and routes, the results of each analysis are the basis for the next one, which makes necessary the analysis of all flights to be able to filter the possible routes and airlines affected in a future step. We would only be able to obtain a pattern of criminal activity with the analysis of the total number of intra-EU flights. And even then, we could not accurately draw a framework of the flow of movement of the targets concerned as a result of a dedicated threat assessment or as a direct result of a checklist.

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

Analyse all intra-EU flights and after "the processing" delete all those data has not risen up a positive result. THIS IS NOT A IDEAL SOLUTION BUT WE WOULD ACCEPT IT IF IS THE CLOSEST APPROACH TO KEEPING INTRA-EU FLIGHTS.

c. Efficiency issues related to fragmentation of data collection

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

In this context is very interesting the methodology, build a platform to share information, request EUROPOL analysis of PNR data and requesting EUROPOL criminal trends and threat assessment is something too very valuable. But the national idiosyncrasy can only be contained by the NCAs. Of course, collaboration/coordination is another utility tool, but the relationship between PIU and NCAs is going to set the course of the investigations. Notwithstanding any other approach at the European level is extremely useful and in the same way, the FYI reports of the EUROPOL template too, but every State is who best knows and understands the criminal circumstances.

The tailored national threat assessment is conducted in a domestic intervention but international support is always welcome in any context and at every level. Thus, we must define very well all the different aspects when it comes to sharing algorithms or formulas in the different criminal types.

On how to align the routes at the European level, it is very difficult to adopt a consensus in this regard, it is not the equivalent of adjusting to a data analysis model through the RBTs or scenarios.

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 MSs? What would be the prerequisites and limitations of such an approach?

Of course, any help or advice is welcome, any piece of information received must be shared with the NCAs to create more intelligence that could be shared in the same way among others PIUs and NCAs.

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

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

First of all, concerning the creation of a third independent authority having the reference of the DPO, we consider that it is a difficult figure to define and difficult to create. We already have two previous authorities: the PIU itself and the DPO. Moreover, it is against the Directive to ask for authorization to share data less than six months old.

But if this figure has to be created (clearly defining its profile and functions) we would assume this fact and above all for the sake of prevailing internal flights.

The possibility of exchanging information is something we support completely but the positions of different delegations are so wide regarding the possibility to select routes and flights that it seems very difficult that the solution could satisfy the demand for any specific route and flight by another PIU.

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

Indeed, this option would only be feasible if the flight data could be kept for a period of six months, but taking into account the Court's approach, we would not be able to share data since it would be very difficult to coincide in the requests of the persons and the flights searched due to fact that rarely two countries coincide on the same person or in the same period with the same airline.

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

At the last meeting, Spain explained that if we override the doubts and prejudices emanating from the Court's ruling we could comply with the spirit of the ruling. That is why working on a protocol to remove those doubts about the privacy of PNR data could be considered a complete solution: a protocol of communications with the NCAs to validate all the results transmitted.

But if we work in the way the Court pretends we can almost certainly say that it will be very difficult or almost impossible to be able to carry out moderate operative police work.

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

In line with the previous explanation, this question would not be necessary.

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

e. Review of selecting intra-EU flights

1.e. Do all delegations share this understanding?

Under the condition to have a third-party authority, to be able to check that the collection of all the intra- EU data is being properly used, we would accept it, but with the involvement of a designated DPO.

2. <u>Retention of PNR data</u>

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?

It is not a matter of re-asses PNR data already received, because terrorism investigations are very long term and data that seemingly do not make sense on first reading within the first six months, but take on meaning with new information obtained and a new review in the following years.

This explanation was very much present in the PNR defence in court when the US-Canada agreement was on trial. OC investigations are earlier and their results are not as long-term, although they also exist.

The solution is not to limit police investigative powers to guarantee data protection but to guarantee data protection without losing police effectiveness.

In any case, Spain could accept a shortening of the deadlines in the benefit of preserving the intra-flight data. Six months would still be a very short period of time, but it would be satisfactory enough if the basis of all intra-flights were kept. The new findings are a prerequisite for future investigations which give much clearer results.

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

2.c. What other observations should be made?

3. <u>Flights within the territory of a single Member State</u>

This is not applicable in Spain. Under the current national legislation, it is permitted to ask for different PNR data by the NCA to the PIU when is duly reasoned and in special situations.

4. Criteria for selecting risk person

Not only in the cases foreseen in article 6 2 a) and c) and 6 3 b) but in 6 3 a) a protocol would be applicable that would result in a subsequent check by the NCAs to be able to verify the false positives and thus, be able to avoid any abuse or any other guideline marked in the sentence.

For Spain the whole sentence is marked by this fear of deployment of PNR data through police databases without any protection and without measures that can guarantee its immediate deletion in case it is not linked to information related to terrorism or organized crime. Therefore, we consider that any action before, during and after any analysis or filtering is welcome as long as the intra-EU PNR data is maintained. The solution of a third authority is excessive considering the figure of the DPO but we will assume this condition as explained above in the case it would be necessary.

SWEDEN

1.a.i – terrorist threat

In Sweden the strategic threat level for 2022 has been ascertained to be elevated, which corresponds to level three on a five-point threat level scale. According to the judgement (paragraph 171), collection of PNR data from all intra-EU flights may only occur on the basis of an assessment carried out by a Member State, establishing that there are sufficiently solid grounds for considering that the Member State is confronted with a terrorist threat which is shown to be genuine and present or foreseeable. It could be argued that the fact that the threat level is elevated is, in itself or in addition to other pieces of information, solid ground for considering that the terrorist threat is genuine and present or foreseeable. However, there is yet no final Swedish position regarding the possibility to continue collecting PNR data from all intra-EU flights.

1.a.ii – filter

The filter option described is an interesting solution which requires further analysis.

1.b.i and ii – Selecting intra-EU flights

The Presidency's idea about limiting the collection of PNR data at the PIUs or other authority has several advantages: 1) it would enable fast connection of new routes, 2) it would prevent the spreading of information about what routes are actually analysed, 3) it is possible that air carriers prefer a single connection process instead of connecting to the PNR system an unknown number of times (depending on what routes are selected) and to take responsibility for delivering the correct data to individual PIU:s. We believe it should be further investigated whether such an elimination function at the PIU could be a viable solution.

1.c.i and ii – Selection of flights and risk assessment

The Swedish PIU would in principle be willing to share risk assessments and to work towards a common methodology. However, the PIU does not normally prepare the risk assessments itself, this is done at the competent authorities working with intelligence or crime investigations. The competent authorities would normally not share their risk assessments with the PIU. Hence, the PIU would not be able to share risk assessments with other PIU:s.

1.d.1 – Sharing of information from intra EU-flights

Our reading is that the judgement does not stop Member States from sharing information and there is no obligation for Member States to select routes bilaterally. However, information exchange must be verified on a case-by-case basis.

1.d.ii - Independent prior review of requests

We share the conclusion that an independent prior review of request is necessary also if the request concerns PNR data in their original form (during the initial 6-months period).

1.d.iii – Sharing of information from selected flights

Sharing information about selected flights would be desirable, but decisions have to be taken on a case-by-case basis due to the sensitivity of the information. PIU:s would have to accept a certain degree of increased administrative burden.

1.d.iv and v – Frequency of selection review and extension to new routes

It is probably necessary for the PIU to review the selection of intra-EU flights on a continuous basis in co-operation with the competent authorities. It seems reasonable to start collecting PNR data from new routes provided that they share the characteristics that form the basis for the selection of other routes.

1.e – Independent review of selection of flights

We share the understanding that decisions that lead to data collection from all intra-EU flights must be subject to review by a court or other independent body. We also share the understanding that Member States have greater flexibility to decide which body shall review the assessments that lead to a selection of intra-EU flights. However, it should be recalled that even if the Member State has a greater flexibility as regards the review of selected flights it still has to assess whether the processing of PNR data is strictly necessary.

2.a – Retention period and assessment of data

The wording "any other circumstance" gives room for a wide interpretation of what could present objective evidence of a risk. This widely formulated criteria in combination with the fact that only an indirect objective link with the carriage of passengers by air is required, could indicate that suspicions of crime or intelligence information may present such evidence of a risk. As regards new pre-determined criteria, our view is that the judgement does not prohibit use of such criteria to reassess already stored PNR data.

2.b – Direct or indirect link

We have no further examples of a direct or indirect link with carriage of passengers by air.

2.c – Standards of evidence for data retention and for access to retained data

We have no other observations to add at this stage.

3.1 and 3.2 – Flights within the territory of a single Member State

Our opinion is that the PNR directive does not apply to domestic flights and the Swedish legislation implementing the directive does not cover domestic flights. There is currently no plan to change this.

4.a and 4.b – Information to data subjects

Providing general information at the time of booking would be a possible way of complying with the judgement. The information that is already provided today could be supplemented by a clarification that any decision to process PNR data has to be evaluated manually. The information could also be supplemented by a description of the general conditions that criteria have to fulfil, as well as information on criteria that cannot be used (race or ethnic origin, political opinions etc.).

However, it would be impossible to disclose any information about specific assessment criteria or methods. It would also be inappropriate to communicate specific information to individuals. This would harm the work of law enforcement authorities and the likely result would be that competent authorities would stop using PNR information.