Ref. Ares(2021)6679191 - 29/10/2021

EUROPEAN
COMMISSION

Brussels, 24.7.2020
SWD(2020) 128 final

COMMISSION STAFF WORKING DOCUMENT

[…]

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and proesecution of terrorist offences and serious crime

{COM(2020) 305 final}

Contents

1. INTRODUCTION 2
2. GENERAL CONTEXT 4
3. ESTABLISHMENT OF AN EU-WIDE PNR MECHANISM 7
3.1. Baseline and EU support measures 7
3.2. General state of play of implementation 8
3.3. Passenger Information Units 9
3.4. Air carrier connectivity 10
3.5. Processing of PNR data 11
3.6. Involvement of competent authorities 12
4. COMPLIANCE WITH PROTECTION STANDARDS IN THE DIRECTIVE 14
4.1. Strict limits on the purpose of processing 14
4.2. Appointment of a data protection officer 16
4.3. Oversight by an independent supervisory authority 17
4.4. Push method 18
4.5. Data security and audit trail 18
4.6. Data retention and de-personalisation 19
4.7. Prohibition of processing of sensitive data 20
4.8. Manual review of matches obtained by automated means 20
4.9. Passengers' rights concerning the use of their data 21
4.10. Stricter conditions on transfer of data to non-EU countries 22
5. OTHER ELEMENTS OF THE REVIEW 23
5.1. The necessity and proportionality of collecting and processing PNR data 23
5.2. The length of the data retention period 30
5.3. The effectiveness of exchange of information between the Member States 33
5.4. The quality of the assessments including with regard to the statistical information gathered pursuant to Article 20 36
5.5. Feedback from Member States on the possible extension of the obligations and the use of data under the PNR Directive 37
6. KEY OPERATIONAL CHALLENGES 41
6.1. Reliability of PNR data 41
6.2. Challenges identified by the air industry 43
6.3. Scope/restrictive purpose limitation 44
6.4. Cross-checks against the SIS and other instruments 46
6.5. Requests from third countries 47

1. INTRODUCTION

Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (henceforth 'the PNR Directive')[1] was adopted by the European Parliament and the Council on 27 April 2016. The Directive regulates the collection, processing and retention of PNR data in the European Union and lays down important safeguards for the protection of fundamental rights, in particular the rights to privacy and the protection of personal data. The deadline for Member States to transpose the Directive into their national law was 25 May 2018.

PNR data are unverified information provided by passengers and collected by air carriers to enable the reservation and check-in processes. The commercial and declaratory nature of PNR distinguishes this type of data from Advance Passenger Information (API) – basic information on the passenger's and the crew's identity, gathered during the check-in process and usually available in the machine readable zone of travel documents, which carriers would generally only collect if there is a legal requirement.[2]

The content of PNR data varies depending on the information given by the passenger and may include, for example, dates of travel and travel itinerary, ticket information, contact details like address and phone number, travel agent, payment information, seat number and baggage information. The analysis of such information can provide the authorities with important elements from a criminal intelligence point of view, allowing them to detect suspicious travel patterns and identify associates of criminals and terrorists, in particular those previously unknown to law enforcement authorities.

Accordingly, the processing of PNR data has become a widely used law enforcement tool, in the EU and beyond, to prevent and fight terrorism and other forms of serious crime, such as drugs-related offences, human trafficking, and child sexual exploitation. In the EU, less than two years after the transposition deadline, the PNR Directive has already proved its necessity in the effort to achieve an effective and genuine Security Union that duly protects the rights and freedoms of citizens.

---

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.

2 In the EU, the collection of API by air carriers and its transmission to the authorities is regulated by Council Directive 2004/82/EC, also known as the 'API Directive' (OJ L 261, 6.8.2004, p. 24). The Directive concerns the use of API data for the purposes of improving border controls and combating irregular immigration, with their use for law enforcement purposes allowed under national law.

This document, which accompanies the Commission's review report on the implementation of the PNR Directive, contains more detailed information and analysis supporting the findings of the review report. As required in Article 19 of the Directive, the review covers all the elements of the Directive, with a particular focus on specific aspects. These aspects are: compliance with the applicable standards of protection of personal data, the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, the length of the data retention period, the effectiveness of exchange of information between the Member States and the quality of the assessments including with regard to the statistical information gathered pursuant to Article 20 of the Directive.

In this respect, section 2 of the document describes the context setting the background for the implementation of the Directive, while section 3 provides a general overview of the steps taken in the development of the EU-wide PNR mechanism. Section 4 focuses on a particularly important dimension of the Directive's implementation, namely compliance with the applicable data protection requirements, with other key elements of the assessment laid down in Article 19 being addressed in section 5. The document also contains – in section 6 – an overview of the main issues and challenges encountered in the implementation and practical application of the Directive.

Evidence for the review was gathered through a variety of sources of information and targeted consultation activities, including statistical data collected by national authorities pursuant to Article 20 of the Directive; the deliverables of the compliance assessment of the PNR Directive commissioned by the Commission;[3] discussions with national authorities and the travel industry within the framework of regular meetings and dedicated workshops on the implementation of the Directive; and field visits to six selected Member States.[4] In order to illustrate how PNR data are used in combating terrorism and serious crime, where possible, the report refers to real life examples provided by national authorities drawing on their operational experience.

---

[3] The compliance assessment, carried out by Milieu Law and Policy Consulting under the supervision of the Commission, was completed on 5 September 2019 and covered the 23 Member States which notified full transposition of the Directive by 10 June 2019 (AT, BE, BG, CY, CZ, DE, EE, EL, FR, HR, HU, IE, IT, LT, LU, LV, MT, PL PT, RO, SE, SK, UK). The assessment of the transposition measures adopted by FI and NL, which notified full transposition after 10 June 2019, and by SI, which notified only partial transposition, is still ongoing. For FI and NL the contractor has only provided the initial results to the Commission. The assessment takes into account both the national legislative measures adopted to transpose the Directive and their practical application. The information on the practical application was gathered via a questionnaire sent to national authorities, including the Data Protection Officers working at the Passenger Information Units.

[4] Field visits were conducted in BE, BG, DE, FR, LV and NL..

This document should not be considered as an exhaustive overview of the conformity and completeness of national transposition measures. Such a detailed analysis of the national measures adopted to transpose the Directive has been carried out within the framework of the aforementioned compliance assessment. Nonetheless, the review will contribute to inform the next steps to be taken by the Commission in relation to the EU internal PNR policy, including the actions necessary to ensure that all Member States' national transposition measures are in full compliance with EU law.

2. GENERAL CONTEXT

In recent years, an increasing number of countries – not limited to the EU Member States – and international organisations have recognised the value of using PNR data as a law enforcement tool. The establishment of a PNR mechanism and the implementation of the PNR Directive should be seen against the background of this broader international trend.

The terrorist attacks which took place in the United States in 2001, Madrid in 2004 and London in 2005 resulted in the adoption of new measures, including legislative instruments on the collection and exchange of PNR data. To set out the elements of the EU's external PNR policy, the Commission presented a first Communication 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries' in 2003,[5] which was reviewed in a Communication adopted in 2010.[6] The 2010 Communication established a set of general criteria to be fulfilled by future bilateral PNR agreements, including, in particular, a number of data protection principles and safeguards.

These general criteria formed the basis of the renegotiations of the PNR agreements with the U.S., Australia and Canada, leading to the conclusion of new PNR agreements with the U.S.[7] and Australia[8] in 2012. These agreements provide for the transfer of PNR data by airlines on flights to and from the EU so that such data can be used in the fight against terrorism and serious transnational crime, while including safeguards for the protection of privacy and personal data. Joint evaluations of these two agreements were launched in the summer of 2019 to assess their wider functioning, operational value and necessity.

---

5 COM(2003) 826 final of 16 September 2003.

6 COM(2010) 492 final of 21 September 2010.

7 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 5.

8 Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, p. 4.

In 2014, the European Parliament requested an opinion from the Court of Justice of the EU as to whether the envisaged agreement between the EU and Canada was compatible with the Treaties and the Charter of Fundamental Rights and, as a result, the draft agreement did not enter into force. On 26 July 2017, the Court of Justice concluded in its Opinion 1/15 that the agreement could not be concluded as intended because several of its provisions were incompatible with the fundamental rights recognised by the EU, in particular the right to data protection and respect for private life.[9] Following the Court's Opinion, new PNR negotiations with Canada were launched in June 2018. In July 2019, the EU and Canada welcomed the successful conclusion of these negotiations and emphasised their commitment to finalise the agreement as soon as possible, subject to Canada's legal review of the text.[10] While Opinion 1/15 concerns formally only the envisaged PNR agreement with Canada, the Commission is working closely with its other international partners to ensure compliance of international PNR data transfers with the Treaty and the Charter of Fundamental Rights, including in the context of the joint evaluations of the existing agreements referred to above.

As for other third countries, following a Recommendation of the Commission, the Council authorised the opening of negotiations with Japan for the signature of a PNR agreement.[11] The negotiations with Mexico, launched in July 2015, are currently at a standstill.

On 6 November 2007, the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.[12] Upon entry into force of the Treaty on the Functioning of the EU on 1 December 2009, the Commission proposal, not yet adopted by the Council, became obsolete. In February 2011, the Commission tabled a proposal for a Directive[13] and, as noted above, this was adopted by the European Parliament and the Council in April 2016. The Commission has supported the implementation of the Directive through the adoption of funding measures,[14] an Implementation Plan[15] and an Implementing Decision[16] regulating the use of data formats and transmission protocols, on which further details are provided below in section 3.4.

---

9 Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592.

10 EU-Canada Summit joint declaration, Montreal 17-18 July 2019.

11 EU-Japan PNR agreement: Council authorises opening of negotiations, 18 February 2020 (available at: https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU-Japan+PNR+agreement%3a+Council+authorises+opening+of+negotiations).

12 COM(2007) 654 final of 6 November 2007.

13 COM(2011) 32 final of 2 February 2011.

14 Information on the funding allocated to Member States for the development of their PNR systems can be found in the Annex to the Implementation Plan to the PNR Directive.

15 SWD(2016) 426 final of 28 November 2016.

Also in 2016, the EU modernised its legislation on protection of personal data through the adoption of Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR)[17] and Directive (EU) 2016/680 (the Law Enforcement Directive on data protection).[18] These legislative acts ensure the effective protection of the fundamental right to data protection enshrined in primary law. [19] On 24 June 2020, the Commission adopted a Communication on aligning the former third pillar instruments with the data protection rules[20] and published the results of the first review and evaluation of the GDPR.[21]

In this context, it should be noted that the Belgian Constitutional Court has made a reference for a preliminary ruling to the Court of Justice on the PNR Directive.[22] The Belgian court has expressed doubts as to the interpretation of certain provisions of the PNR Directive and their compliance with the Charter of Fundamental Rights and the Treaty. Recently, a reference for a preliminary ruling has also been made by the Cologne District Court.[23]The Commission has submitted observations in the first of these proceedings and will do the same in the second in due course.

At the global level, in December 2017 the United Nations Security Council adopted resolution 2396 (2017) requiring all UN States to develop the capability to collect, process, and analyse PNR data and to ensure that PNR data are used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms.[24] The scope of the Resolution, focused primarily on terrorism, was then extended to organised crime by Resolution 2482 (2019).[25] Against this backdrop, the International Civil Aviation Organisation (ICAO) has started working on the development of a standard for the collection,

---

16 Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units, OJ L 113, 29.4.2017, p. 48.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1.

18 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

19 In particular, Article 16 of TFUE guarantees the right to protection of personal data. This right is also enshrined in Article 8 of the EU Charter of Fundamental Rights.

20 COM (2020) 262 final of 24 June 2020.

21 COM(2020) 264 final of 24 June 2020.

22 Request for a preliminary ruling in Case C-817/19 *Ligue des droits humains*, OJ C 36, 3.2.2020, p. 16–17 (pending).

23 Request for a preliminary ruling in joined Cases C-148/20, C-149/20 and C-150/20 *Deutsche Lufthansa*, not yet published (pending).

24 Resolution 2396 (2017) - Adopted by the Security Council at its 8148th meeting, on 21 December 2017.

25 Resolution 2482 (2019) - Adopted by the Security Council at its 8582nd meeting, on 19 July 2019.

use, processing and protection of PNR data. A Union position on this matter was agreed by means of a Council Decision (EU) 2019/2107 of 28 November 2019 with a view to ensure compliance with the applicable Union legal framework.[26] The Commission has actively engaged in this process, as an observer representing the EU, to ensure the compatibility of these standards with the EU legal requirements, so that they can contribute to facilitate transfers of PNR data. A draft version of the PNR standards was approved by the ICAO Facilitation Panel in February 2020 and sent to the ICAO Contracting States for consultation. After a final review by the ICAO Air Transport Committee, the standards were adopted by the ICAO Council on 23 June 2020. These standards will be binding on all ICAO member countries unless they file a difference.

3. ESTABLISHMENT OF AN EU-WIDE PNR MECHANISM

3.1. Baseline and EU support measures

It should be borne in mind that, before the adoption of the Directive, most Member States did not have a pre-existing system for the collection and processing of PNR data and had to build their capabilities from scratch. The Implementation Plan,[27] adopted by the Commission on 28 November 2016, acknowledged the challenges in terms of resources, time and technical difficulty in setting up PNR systems compliant with the Directive. The plan provided guidance to the Member States by identifying the key steps and measures that needed to be taken in order to set up an operational PNR system.

The Commission has supported the Member States throughout the whole implementation process by coordinating regular meetings, facilitating the exchange of best practice and peer-to-peer support, and providing financial assistance.

In particular, to support the implementation of the PNR Directive, the Budgetary Authority reinforced the 2017 Union budget with EUR 70 million for the Internal Security Fund-Police (ISF-Police), specifically for PNR-related actions.[28] The Commission has also funded four

[26] OJ L 318, 10.12.2019, p. 117. The position of the Union and its Member States has also been set out in an information paper on 'Standards and principles on the collection, use, processing and protection of Passenger Name Record data' that was submitted to the 40th Session of the International Civil Aviation Organisation Assembly.

[27] Commission Staff Working Document, Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SWD(2016) 426 final, 28.11.2016.

[28] This financial assistance has been distributed among the Member States according to the ISF-Police standard distribution key – i.e. 30% in relation to population, 10% in relation to territory, 15% in relation to number of sea and air passengers, 10% tons of cargo (air and sea), 35% as inverse proportion to GDP.

PNR-related projects under the Union Actions of the ISF-Police. These projects aimed to ensure that the Passenger Information Units of the Member States developed the capabilities needed to exchange PNR data or the results of processing such data with each other and with Europol.

The first of these projects was the 'Pilot programme for data exchange of the Passenger Information Units', or 'PNRDEP'. The project, coordinated by Hungary and implemented from February 2016 to June 2017, was awarded EUR 1.15 million to look into the possibilities facilitating the exchange of PNR data between the Passenger Information Units and Europol. It was followed by the PIU.net project, which was coordinated by the Netherlands and implemented from November 2017 to September 2019, with a grant of EUR 3.78 million. Its objective was to deliver a technical solution that would facilitate the exchange of PNR data between the Passenger Information Units. A third project, led by Hungary under a EUR 855,000 grant (currently ongoing), focuses on developing and providing training for PNR practitioners in the Member States. In addition, Germany is currently coordinating a project that focuses on exploring the means to enhance the interoperability of PNR data with IT systems of law enforcement authorities at both national and EU level, with a budget of EUR 2.61 million.

These funding measures are in addition to the grants awarded under the Call for Proposals PNR 2012 within the Specific Programme for Prevention of and Fight against Crime (ISEC) 2007-2013, which overall amounted to EUR 37 million[29] and aimed to help implement national schemes based on domestic PNR legislation adopted prior to the adoption of the PNR Directive.

3.2. General state of play of implementation

Article 18.1 of the PNR Directive requires Member States to adopt measures necessary to comply with the Directive by 25 May 2018. As of 25 May 2020, the end date of the review period, 24 out of 26 Member States[30] had notified full transposition to the Commission. The Commission has not hesitated to make use of its competences as the guardian of the treaties to ensure that Member States comply with their obligation to transpose the Directive. On 19 July

[29] The final amounts paid to the Member States are lower than the maximum amounts foreseen in the initial grant agreements and described in the PNR Implementation Plan because they reflect only the costs incurred by the Member States in the implementation of their PNR projects which were considered eligible.

[30] Denmark, by virtue of Protocol 22 to the Treaties, does not participate in measures proposed pursuant to Title V of Part Three TFEU, including the PNR Directive. Therefore, for the purpose of this report all "Member States" should be understood as referring to all EU Member States except Denmark. The United Kingdom, as a Member State, was bound by the PNR Directive until 31 January 2020.

2018, the Commission initiated infringement proceedings, sending letters of formal notice to fourteen Member States that had failed to communicate full transposition. In ten of these cases, the infringement proceedings were closed in light of a subsequent notification of full transposition of the Directive.[31] Spain, which has not notified any transposition measures, was referred to the Court of Justice for failure to implement the Directive on 2 July 2020. Regarding the remaining three Member States, the Commission will decide how to proceed in the coming months.

In addition, most Member States have reached the key milestones identified in the Implementation Plan and have operational PNR systems in place. Considering the complexities surrounding the deployment of PNR systems and the limited time available, the operational successes achieved by Member States can be considered as a significant achievement. Further details on the main aspects of the implementation process are provided below.

3.3. Passenger Information Units

The Passenger Information Unit is the core of the PNR mechanism. The Passenger Information Unit is a dedicated unit set up to receive PNR data from the air carriers. Each Member State must establish a Passenger Information Unit (Article 4.1). The Passenger Information Unit is the 'guardian' of the PNR database, in the sense that only its staff should have access to all the PNR data collected. The Passenger Information Unit is responsible for conducting the initial assessment of PNR data and sending the results of their processing to law enforcement authorities at the national level (the 'competent authorities', in the Directive's terminology) as well as for exchanging PNR with the Passenger Information Units of other Member States and with Europol (Article 4.2). Member States are also required to adopt a list of competent authorities entitled to request or receive PNR data and the results of processing such data from the Passenger Information Unit.

All Member States have established their Passenger Information Units, which – as noted above – are central to the EU PNR architecture.[32] In every Passenger Information Unit except one, a Data Protection Officer has already been appointed to monitor the lawfulness of data processing and the compliance with data protection safeguards.

---

[31] AT, BG, CY, CZ, EE, EL, FR, LU, PT, RO. This decision was based on the Commission's assessment of the completeness of national transposing measures, but does not prejudge the result of the assessment of their conformity.

[32] The list of established Passenger Information Units has been published in the Official Journal and can be consulted here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XC0702%2802%29

3.4. Air carrier connectivity

Air carriers collect and process PNR data for their own commercial and business purposes, independently of the provisions of the PNR Directive. Importantly, the Directive does not oblige air carriers to collect or retain data from passengers, nor the passengers to provide any additional data to air carriers. At the same time, the Directive stipulates that pre-defined data categories collected by airlines in the course of their normal business must be transmitted to the Passenger Information Unit of the Member State of arrival or departure.

Enabling data transfers from air carries to national authorities requires lengthy preparations. The process necessary to connect air carriers' reservation systems to the IT systems of national Passenger Information Units is multi-faceted and involves, among other actions, engaging with air carriers (up to 180 different carriers for a single Member State), establishing IT connections with airlines and the companies managing their reservation systems, and testing the provision of PNR data.

To facilitate this process, on 28 April 2017, the Commission adopted the Implementing Decision (EU) 2017/759[33] establishing a common list of protocols and data formats from which carriers may choose for the purposes of conducting PNR data transfers. The Implementing Decision is based on the ICAO guidelines on PNR,[34] and the international standards developed by ICAO, the International Air Transport Association (IATA) and the World Custom Organisation (WCO) for the transmission of API and PNR data by airlines to government authorities.[35] Member States were required to take the necessary measures to apply the Implementing Decision by 28 April 2018. This means that, as of this date, Member States had to ensure that carriers should be able to use the data format and transmission protocol of their choice – among those listed in the Implementing Decision – when transferring PNR data to the Passenger Information Units. At this stage, the process to ensure carrier connectivity is still ongoing, and the coverage in terms of passenger flows and flights differs across the Member States. The experience of Member States that are the most advanced in the implementation process shows that it takes time to achieve broad levels of coverage, in particular regarding the establishment of connectivity with small carriers.

---

33 Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units, OJ L 113, 29.4.2017, p. 48.

34 ICAO Document 9944, 'Guidelines on Passenger Name Record (PNR) Data', 2010.

35 Available at the ICAO website: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx.

In general, a collaborative approach permeates the relationships between the authorities and the industry. Whereas all Member States have included in their national legislation sanctions for carriers who fail to transfer PNR data as required under the Directive, in practice these sanctions have been imposed only exceptionally.

3.5. Processing of PNR data

Under the framework established by the Directive, the processing of PNR data can only be conducted in three ways:

(i) Proactively, to create and update pre-determined criteria[36] according to which future passengers should be subjected to additional scrutiny (Article 6.2(c)). For example, the analysis of PNR data may show that a certain travel route is particularly likely to be used by drug traffickers and this information can be used proactively to build new targeting rules, or refine existing ones.

(ii) In real-time, to assess the passengers prior to their scheduled arrival in or departure from a Member State, by comparing PNR data against pre-determined criteria and relevant databases – for example, the Schengen Information System (SIS) or national watch lists – in order to identify individuals who should be subject to further examination by the authorities (Article 6.2(a)).

(iii) Reactively, responding to 'duly reasoned' requests, on a case-by-case basis in compliance with the legal requirements of the Member State, from the competent authorities within the framework of criminal investigations (Article 6.2(b)).

Any positive matches obtained when comparing PNR data against pre-determined criteria and databases must be individually reviewed by no-automated means to verify whether the competent authority needs to take action under national law (Article 6.5). The underlying principle is that no decisions that produce an adverse legal effect on a person or significantly affect that person should be taken only by reason of the automated processing of PNR data, without human intervention. Most Member States are now able to process PNR data against databases and watch lists relevant for the purposes of the Directive. Apart from the use of national law enforcement databases, a large majority of Passenger Information Units also

[36] Pre-determined criteria, also known as targeting rules, are search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers which corresponds to certain abstract profiles, e.g. passenger travelling on certain routes commonly used for drug trafficking, who bought their ticket in the last moment and paid in cash, etc.

compare PNR data against relevant EU and international data repositories, such as the SIS and the Interpol's Stolen and Lost Travel Document database.

The use of pre-determined criteria – more demanding from the operational, analytical and technical point of view – is still at an early stage of implementation in some Member States. Since January 2020, Europol provides assistance to the Member States in the development of this processing method through its Travel Intelligence Task Force. The Task Force centralises, analyses and distributes relevant information and intelligence on patterns, trends and modus operandi which can be used by the Member States' Passenger Information Units to develop targeted, proportionate and specific targeting rules. Training on the development of pre-determined criteria is also supported through an ongoing EU-funded project, financed under the ISF-Police Union Actions.[37]

Member States have reported that PNR processing has already actively contributed to their successes in the prevention and fight against terrorism and other serious forms of criminality, often committed by organised criminal groups. PNR has been found to be particularly effective to combat drug trafficking, terrorism-related offences, human trafficking and child sexual exploitation, fraud and money laundering.[38] The feedback provided by national authorities indicates that it is difficult to determine which processing method (i.e. comparison against databases, watch lists or the use of targeting rules) is the most useful or efficient. In many cases, the best results are obtained from a combination of all the various processing methods available.

3.6. Involvement of competent authorities

Article 7 of the PNR Directive requires Member States to 'adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the Passenger Information Unit'. It also provides that such authorities 'shall be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime'. All Member States have already established a list of competent authorities and notified it to the Commission.

Almost all Member States have appointed the police and other relevant authorities for crime prevention and the protection of public order as competent authorities. In addition, national transposition measures in many Member States designate intelligence services, including

[37] For more details on this project, see section 3.1.

[38] More detailed information about the use of processing methods and results obtained may be found in section 5.1.

military intelligence services, as authorities competent to receive and request PNR data from the Passenger Information Unit.[39] Less than half include the judicial authorities on their list of competent authorities, mainly the State Prosecutor's Office and, in some cases, the courts. The vast majority of Member States have also designated customs as a competent authority, whereas only a few have done so for the financial authorities (when responsible for investigation of fraud, money laundering or other financial crimes).[40]

In principle, Member States have assessed the cooperation between the Passenger Information Units and competent authorities in positive terms, although both parties needed time to familiarise to the new tool and to develop cooperation methods. Most Member States have made use of the possibility to second staff from the competent authorities to the Passenger Information Units and report that this has resulted in the sharing of experiences and facilitated the development of closer relations.

National authorities have also reported that, in the first months of the Passenger Information Units operational activities, competent authorities might have lacked sufficient awareness as to how PNR data may be used and, as a result, the requests submitted were too broad in scope or not sufficiently justified. In most cases, these problems were solved through dialogue and training. In addition, many Member States use a template for requests, which guides the competent authorities as to the elements that need to be included thereto, thus facilitating the procedure. All Passenger Information Units have observed a significant growth in the number of requests received from the authorities over a short period of time. This clearly shows that law enforcement authorities are increasingly aware of the tool and find it useful.

Investigations on serious crime and terrorism are a multi-stage process, with information coming from various sources. Therefore, it may be difficult to single out the exact impact that the use of PNR data has had in each specific case. However, law enforcement authorities from across Member States have indicated that PNR data has been successfully used to organise and plan operational and monitoring activities in advance, obtain full details of persons of interest, identify previously unknown suspects, establish links between members of crime groups through the analysis of contact and payment details, and verify the assumed 'modus operandi' of serious criminals and organised crime groups. In addition, the establishment of

[39] This is compatible with the PNR Directive to the extent that these services use PNR data only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime (Article 7.4), i.e. respecting the purpose limitation of the Directive.

[40] The list of competent authorities, as notified to the Commission by each Member State, has been published in the Official Journal and can be consulted here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XC0606%2801%29

the EU PNR mechanism has enhanced the authorities' ability to trace the movement of persons subject to a criminal investigation (in particular within the Schengen area) and determine the travel patterns of criminal suspects.

An outstanding issue in some Member States concerns the limited feedback provided by the competent authorities to the Passenger Information Unit following the transfer of data to them. The staff of the Passenger Information Units consider such feedback necessary to better align the processing methods with the needs of law enforcement services. The unwillingness to provide feedback has been explained by confidentiality requirements, data protection concerns[41] and the fact that many investigations are not necessarily concluded immediately after the transfer of PNR data.

4. COMPLIANCE WITH PROTECTION STANDARDS IN THE DIRECTIVE

A key objective of the Directive is to ensure that the processing PNR data by national authorities is carried out in a manner compatible with the fundamental rights of all passengers. The Directive therefore regulates the way in which Member States can use PNR data transferred by airlines and establishes a number of strict data protection safeguards. This section provides a comprehensive overview of these safeguards and their implementation by the Member States. Whereas the results of the compliance assessment already available to the Commission show an overall compliance with these safeguards, instances of non-conform transposition have been identified. The Commission is committed to ensuring full conformity of transposition and hence will not hesitate to pursue infringement action, if necessary, once the compliance assessment is finalised.

4.1. Strict limits on the purpose of processing

Under the Directive, PNR data can only be used by national law enforcement authorities for preventing, detecting, investigating and prosecuting terrorism and serious crime (Article 1.2). The definition of terrorist offences is further specified by referring to Framework Decision 2002/475/JHA,[42] now replaced by Directive (EU) 2017/541 (Article 3.8).[43] A list of offences regarded as serious crimes is provided in Annex II to the PNR Directive. To be under the

[41] One Member State reported that competent authorities considered that providing feedback to the Passenger Information Unit on individual cases would amount to processing of personal data, for which there was no basis in national law.

[42] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3.

[43] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6.

scope of the Directive, these offences must be punished with a maximum term of at least three years of imprisonment (Article 3.9).

Concerning the processing of PNR data, the Directive specifies that the data can only be compared against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert or processed against pre-determined criteria (Article 6.3). In addition, competent authorities may only request and process PNR data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime (Articles 6.2(b) and 7.4 PNR Directive).

Most Member States comply with the strict purpose limitation requirements of the Directive and limit the processing of PNR data to the purposes specified in Article 1.2. Four Member States have adopted national measures that go beyond the purpose limitation, by specifically allowing the use of PNR for national security purposes.

National transposition measures regulate the processing of PNR data against databases and pre-determined criteria in accordance with the requirements and limitations set out in Article 6 of the Directive.[44] In particular, the requirement to only use the databases relevant for serious criminal offences and terrorism is explicitly reiterated in the national PNR laws of all Member States, except two.

National authorities consider that the purpose limitation stipulated by law and the ensuing restrictions with regard to processing methods are crucial tools to ensure that PNR data are processed in accordance with the Directive. In terms of application, national authorities follow different practical approaches to ensure respect for the Directive's purpose limitation. One such practice requires that the design of targeting rules is properly documented and that the rules themselves are thoroughly tested against historical data, to exclude those that generate matches considered outside the Directive's scope. Some Member States compare PNR data only against the specific sections or alert categories in law enforcement databases that are considered more relevant for the purposes of the PNR Directive, and require the Passenger Information Unit to refrain from forwarding hits for offences that are not covered by them.[45] The provision of training to competent authorities and the use of templates for PNR data requests also helps to ensure that the authorities in question have an adequate understanding of the purposes for which PNR data can be used.

[44] For more details on the compliance with the conditions of the use of pre-determined criteria, see below.
[45] For a more detailed overview of this issue, see Section 6.3.

4.2. Appointment of a data protection officer

The Directive requires the Member States to appoint a Data Protection Officer to monitor data processing and to implement necessary safeguards (Article 5.1). Member States are also required to provide Data Protection Officers with the means to do their work effectively and independently. Data Protection Officers have a number of important functions such as acting as a single contact point for passengers with concerns related to PNR data (Article 5.3), being informed of PNR data transfers to third countries (Article 11.4) and conducting an ex post review of unmasking authorisations, unless such authorisation is given by a judicial authority (Article 12.3(b)(ii)). The Data Protection Officer should have access to all the data processed by the Passenger Information Unit and be competent to refer to any instance of unlawful data processing to the national supervisory authority (Article 6.7).

All Member States except one have already appointed a Data Protection Officer to monitor data processing by the Passenger Information Unit and to implement necessary safeguards. The Directive's requirement that the Data Protection Officer shall have the means to perform his or her duties and tasks independently has been mirrored in national legislations. Practically, the degree of independence of the Data Protection Officer can be expected to be greater when he or she is not a member of the Passenger Information Unit staff and is not subordinated to the head of Passenger Information Unit.

According to national authorities, the Data Protection Officers play a major role in the functioning of the Passenger Information Units by carrying out regular controls of the lawfulness of data processing and providing advice to Passenger Information Unit staff on data protection matters. In many Passenger Information Units, the Data Protection Officers also participate in the development and regular review of pre-determined criteria, to ensure that these are proportionate and non-discriminatory (see below for more details). Other tools available to the Data Protection Officers include the possibility to send quarterly reports to the Passenger Information Unit with suggestions for improvement and the provision of training to the Passenger Information Unit staff.

In principle, the right of data subjects to contact the Data Protection Officer as a single point of contact has been provided for by law in all but two Member States. Most Member States also facilitate the exercise of this right by making the contact details of the Data Protection Officer easily accessible, e.g. on the website of the Passenger Information Unit.

The access of the Data Protection Officer to all data processed by the Passenger Information Unit is guaranteed by law in all Member States except one. The control powers of the Data

Protection Officer have in principle been correctly mirrored in national legislation, although several instances of non-conform transposition have been detected. Four Member States do not explicitly recognise the competence of their Data Protection Officers to refer cases of unlawful processing to a national supervisory authority. In addition, the exercise of this competence has been limited in two others, either by restricting it to certain types of cases or by introducing an intermediary procedure, not foreseen by the Directive.

4.3. Oversight by an independent supervisory authority

An independent national data protection supervisory authority must oversee the application of the Directive at the national level with a view to protecting fundamental rights in relation to the processing of personal data (Article 15.1-2). The supervisory authority is responsible for dealing with the complaints of data subjects. All Member States have appointed a national supervisory authority. In most Member States, this authority is provided for under the general law on data protection transposing Framework Decision 2008/977/JHA[46] or Directive (EU) 2016/680 (also known as the Law Enforcement Directive)[47] which repeals and replaces it.

In most Member States, the competences of the supervisory authority to deal with complaints from data subjects, to carry out investigations, to verify the lawfulness of data processing and to provide advice to data subjects have been fully and correctly enshrined in the national legislation. Six Member States reflected most of these competencies, but failed to include all in their laws.

Under the Directive, the Passenger Information Units are also under obligation to report, to the supervisory authority and the person concerned, any personal data breach likely to result in a high risk for the protection of personal data or to affect the privacy of the data subject adversely (Article 13.8). All Members States have transposed this obligation into their national laws, whilst two narrow its scope of application, by limiting the situations in which the data subject must be informed. No data breach has been reported by a Member State thus far.

---

[46] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

[47] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

4.4. Push method

Under the Directive, PNR data should be made available to national authorities through the so-called 'push method' (Article 8). This means that the data must be transmitted by the air carriers to the Passenger Information Unit instead of the Passenger Information Unit obtaining data by accessing the air carriers' reservation systems ('pull method'), which is considered a more privacy-intrusive method.

In line with this requirement, all the Member States provide for data transmissions exclusively by the push method. In addition, all national transposition measures preserve the role of the Passenger Information Unit as the only entity that can receive, process and store PNR data. This is important as it preserves, in all Member States, the function of the Passenger Information Unit as the custodian of the PNR database. As a result, other public authorities have no direct access to PNR data, either when stored in the airlines' reservations systems or at the Passenger Information Unit.

4.5. Data security and audit trail

Member States must implement the necessary technical and organisational measures to ensure that PNR data are processed with a high level of security (Article 13.7). Processing operations – such as the collection, erasure, disclosure and consultation of PNR data – should be logged and documented, so that the supervisory authority can have access the records if necessary, for example, to conduct audits (Article 13.5 and 13.6). These records should be kept for a period of five years and can be used only for the purposes enumerated in the Directive (Article 13.6).

In practice, the confidentiality and security of data processing are ensured by a number of administrative, technical and practical measures. In particular, only the selected Passenger Information Unit staff members have access to PNR data and their activities are monitored. The processing takes place in secure premises and with the use of highly secured IT systems.

All Member States have transposed the obligation to keep records of all processing operations. National authorities have highlighted such logging as an important tool to ensure the lawfulness of data processing within the Passenger Information Unit, in particular because it allows the Data Protection Officers to monitor all the processing operations.

Nevertheless, several instances of non-compliance with the key requirements relating to logs have been identified. Three Member States have failed to correctly transpose all Directive requirements concerning information, which should be recorded, whereas three others

extended the purposes for which the logs can be used. In addition, three Member State have failed to transpose the provision regulating the duration for which logs need to be stored and two others have transposed it incorrectly, either by shortening or extending the period. The obligation to make the logs available to the national supervisory authority has not been transposed by one Member State and was transposed in a non-compliant manner by two others.

4.6. Data retention and de-personalisation

PNR data can be stored in the database of the Passenger Information Unit for five years (Article 12.1). However, after six months the data will be 'masked out' by removing all the elements that may serve to identify a passenger – for example, the name, contact and payment information (Article 12.2). After this, the authorities will only be able to access the full PNR data set (including the elements masked out) under specific conditions (Article 12.3). The reservation details, such as the PNR record locator, date of reservation and travel, the itinerary, travel agency information, code share and luggage information will be still directly available to the user, allowing for data processing for statistical purposes as well as to gather intelligence. Depersonalised data can also be searched and disclosed in the framework of investigations into terrorist and serious criminal activities, with the approval of the designated authorities and following the established procedures.

All the national transposition measures limit the retention period to five years and provide for the depersonalisation of PNR data after six months. Nevertheless, concerning depersonalisation, one Member State has failed to define any data element which should be masked, while five other Member States have failed to include some of the data elements required by the Directive in their national laws.

The requirement to only disclose full PNR data after the expiry of the six-month period when certain conditions are met was correctly transposed by a large majority of Member States. Nevertheless, two Member States have failed to correctly transpose the requirement that the disclosure of full data must be reasonably believed to be necessary for responding to a request according to Article 6.2(b). In all Member States, such disclosure must be approved either by a judicial authority or by another competent national authority. In some Member States, both methods have been used. However, four Member States have failed to correctly transpose the safeguard concerning the need forex-post review by the Data Protection Officer when the disclosure of PNR data has been approved by another competent authority.

4.7. Prohibition of processing of sensitive data

The Directive prohibits the processing of 'sensitive data' – that is, information which could reveal a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation (Article 13.4). In addition, the criteria against which PNR data can be processed, cannot be discriminatory and shall, in no circumstances, be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation (Article 6.4). The principle of non-discrimination also applies to decisions made by national authorities, following the processing of PNR data (Article 7.6).

The prohibition of processing sensitive data was fully transposed by a large majority of Member States, with only two exceptions. In addition, all Member States but one require an immediate deletion of such data, if collected. However, four Member States have failed to transpose correctly the prohibition on the use of discriminatory pre-determined criteria or criteria based on sensitive data. Five Member States did not transpose the obligation that decisions of competent authorities must respect the principle of non-discrimination.

With regard to the practical realisation of the prohibition to collect and process sensitive data, national authorities report that the IT systems of the Passenger Information Unit are designed in a way that makes the collection and processing of sensitive data technically impossible. This means that such data, even if transferred by air carriers, is filtered out and blocked or deleted by the system. In addition, the fact that sensitive data are not collected in practice excludes the possibility of designing pre-determined criteria based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

4.8. Manual review of matches obtained by automated means

Any match obtained through the automated processing of PNR data must be manually reviewed (Article 6.5). For example, the comparison of PNR data with the data stored in a watch list may flag up an individual flying to the Member State for further examination. In this case, the competent staff must review the match to either confirm it or discard it. This is to ensure that no decisions having an adverse effect on an individual (such as being subject to further checks on arrival or departure) are taken without human intervention.

All the Member States have transposed the obligation to verify the matches resulting from automated processing. With regard to practical application, the measures adopted concern, for instance, the technical design of the IT system as well as internal procedures regulating the

functioning of the Passenger Information Unit, which impose the manual verification of matches.

4.9. Passengers' rights concerning the use of their data

Passengers have a right to access their data, rectify them and have them deleted or have their processing restricted. They also have the right to receive compensation for any damage they have suffered and to seek redress before a court (Article 13.1). These rights are further developed in the Law Enforcement Directive.[48] In addition, Member States must ensure that passengers are clearly informed about the collection of PNR data and of their rights.[49]

Most Member States have transposed the provisions relating to data subjects' rights through the national legislation implementing the Law Enforcement Directive. This Directive was transposed either by specific legislation on the handling of personal data by law enforcement authorities for the prevention, detection, investigation and prosecution of certain offences, or by the general law on protection of personal data. However, in three Member States national transposition measures on the PNR Directive do not contain a correct cross reference to the national legislation transposing the Law Enforcement Directive.

With regard to the practical exercise of data subjects' rights, including the obligation to inform the passengers about the collection and processing of their data, national authorities pointed to the fact that relevant information has been made available online, including on the steps to follow to exercise the rights to access, rectification, erasure, restriction, compensation or judicial redress. Many also underlined the role of the Data Protection Officer, acting as a single point of contact, to provide passengers with the information and facilitate the exercise of their rights.

4.10. Stricter conditions on transfer of data to non-EU countries

The transfer of PNR data by the Member States to countries outside the EU is only allowed on a case-by-case basis and when necessary for fighting terrorism and serious crime (that is, exclusively for the purposes for which PNR can be used under the Directive). Furthermore, PNR data may be shared only with public authorities that are competent for combating these kinds of offences (Article 11.1). Importantly, PNR data can only be transferred to non-EU

[48] This Directive has replaced the Framework Decision 2008/977/JHA.

[49] The collection and processing of PNR data by air carriers and their service providers, and the connected rights of data subjects are regulated by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016, p. 1.

countries only under conditions consistent with the PNR Directive and those laid down in the Law Enforcement Directive, and only upon ascertaining that the use the recipients intend to make of the PNR data is consistent with those conditions and safeguards (Article 11.3). The Data Protection Officer should be informed about every transfer of data to a third country (Article 11.4).

All the Member States have established a regulatory framework for PNR data transfers to third countries that mirrors the strict limitations imposed by the Directive. In particular, the requirement that such transfers can only be made on a case-by-case basis has been transposed by all Member States. However, four Member States have failed to fully transpose other conditions provided for by the Directive relating to the purposes for which the data can be transferred or the authorities competent to receive it.

Importantly, the law in all Member States requires that recipient third countries agree that onward transfers to another third country can be made only with the express authorisation of the Member State whose Passenger Information Unit has transferred the data, as required under Article 11.1(c). The Directive also provides that in exceptional circumstances such a transfer can take place also without prior authorisation if certain conditions are met, notably that the transfers are essential to respond to a specific an actual threat related to terrorist offences or serious crime in a Member State or a third country and prior consent cannot be obtained in good time (Article 11.2). These conditions were not fully mirrored in the legislation of eight Member States.

National authorities have pointed to the active role of the Data Protection Officer in the processing of requests received from third countries. However, in two Member States, the transposition of Article 11.4 of the Directive, requiring that the Data Protection Officer be informed each time the Member State transfers PNR to a third country, is not in -conformity as the national transposing legislation restricts the role of the Data Protection Officer. In these Member States, the Data Protection Officer is only informed in case a transfer is carried out without the prior consent of the Member State from which the data were obtained.

5. OTHER ELEMENTS OF THE REVIEW

5.1. The necessity and proportionality of collecting and processing PNR data

Article 19 requires the Commission to assess the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, i.e. (i) to assess the passengers prior to their arrival to or departure from the country; (ii) to respond to a duly

reasoned request from the competent authorities, within the framework of criminal investigations; and (iii) to update and create the pre-determined criteria to be used to identify passengers requiring additional scrutiny by the authorities (see also above section 3.5). The assessment below presents several elements justifying the necessity and proportionality of such processing.

The objectives and effectiveness of PNR processing

Identifying whether PNR processing meets an objective of general interest constitutes an important step in performing a necessity and proportionality assessment. The PNR Directive, and the processing of data which it legitimises, is intended to protect public security by ensuring the prevention, detection, investigation and prosecution of serious crime and terrorism in the area without internal borders existing in the Union. As confirmed by the Court of Justice in Opinion 1/15, the objective of ensuring public security in the fight against terrorist offences and serious crime is an objective of general interest of the Union capable of justifying interference, even serious, with the fundamental rights enshrined in Articles 7 and 8 of the Charter.[50] This conclusion can be reasonably expected to apply to PNR processing operations which serve to ensure public security in the territory of the Union.

In the limited time since the transposition deadline, PNR has proven to be effective in achieving the objective of general interest pursued. According to the Member States, the different types of processing of PNR data available to them (real time, reactive and proactive) have already delivered tangible results in the fight against terrorism and crime. National authorities have also highlighted that these results could not have been achieved without the processing of PNR data, e.g. by using exclusively other tools such as API. Put differently, pre-existing measures were insufficient to achieve the intended objectives. The effectiveness of the various means of PNR processing is further detailed below.

In real-time, PNR data are used – in a similar way to API and in combination with it - to track down individuals known for their involvement in terrorist offences and serious crime. To attain this objective, PNR data are automatically checked before arrival or departure against various law enforcement databases of persons and objects sought. However, unlike API, which is collected at the moment of check-in, PNR data are transferred to Passenger Information Units 48 to 24 hours before the flight scheduled departure. This allows the

[50] Point 149 of the Opinion.

competent authorities more time to prepare a law enforcement action, if necessary, which is often crucial for the success of the intervention.

Even more importantly, PNR data can be used to identify persons involved in criminal or terrorist activities who are, as of yet, not known to the law enforcement authorities. This is because the processing of PNR data can highlight - for a further assessment- passengers whose travel behaviours are atypical or fit the travel patterns usually encountered in the case of offenders. This objective can only be achieved through the use of PNR data. In practice, this is done by comparing PNR data, through automated means, against combinations of predetermined fact-based risk indicators. Examples of such risk-indicators reported by national authorities include the fact that the passengers have booked their tickets using travel agencies known to be used by traffickers or have chosen travel routes that are both longer and more expensive than the routes a person travelling for business or tourism purposes might have chosen. The use of pre-determined criteria may also identify passengers whose luggage does not correspond with the length of the stay and destination, which may raise suspicions of involvement in trafficking of illicit goods or money laundering. Similarly, information that a credit card belonging to a suspected trafficker was used in order to book a ticket for another person might reveal the existence of a form of trafficking, even though the person travelling may not be known to law enforcement authorities. According to the Member States, used in combination with other investigative tools and methods, PNR allows law enforcement authorities to detect suspicious behaviour, better target their investigation, prioritise one lead over the other, build up their case and gather evidence necessary to obtain a conviction.

Without claiming to be exhaustive, Member States have provided examples to the Commission, some of which are quoted at the end of this section, that illustrate how the comparison of PNR data against databases and pre-determined criteria was necessary for the identification of potential perpetrators of acts of terrorism or persons involved in other forms of serious crime, such as drug trafficking, cybercrime, human trafficking, child sexual abuse, child abduction and participation in organised criminal groups. Notably, some cases could not have been solved without the use of PNR data, in particular if there had been no other indication that the suspect might be involved in terrorist or other criminal activities. In some instances, the use of PNR data resulted in the arrest of persons previously unknown to the police services, or allowed for the further examination by the competent authorities of passengers who would not have been checked otherwise. The assessment of passengers prior to their departure or arrival has also helped prevent crimes from being committed.

In addition to real-time processing, national authorities have reported that PNR data retained after the passengers' arrival or departure have also been successfully used in a retrospective manner to support the investigation, prosecution and unravelling of criminal networks after a crime had been committed. In this respect, the analysis of historical data has sometimes been the only tool available to identify individuals involved in certain forms of criminal activity or terrorism or to obtain evidence necessary to prove the guilt of a criminal. The increasing number of case-by-case requests submitted to the Passenger Information Unit by the competent authorities shows that the latter are actively using PNR data in their investigations. Further details and practical examples on the use of PNR data retained in the Passenger Information Unit database are provided in the section on data retention below.

PNR data are also used proactively, i.e. to develop and update pre-determined criteria, which are used for the processing of passengers' data prior to the flight's departure or arrival. National authorities have confirmed that PNR data are indispensable to gain a detailed insight into the travel patterns of those involved in terrorism and serious crime and to develop pre-determined criteria that are proportionate, targeted and specific, as required by the Directive. It is also crucial that the Passenger Information Unit staff are able to quickly detect changes in the criminals' travel behaviour (e.g. the change of routes) and to adapt the criteria accordingly. Again, this aim cannot be achieved to the same extent by relying on other sources of intelligence, making the processing of PNR data necessary. In particular, according to national authorities, the proactive processing of PNR data has been necessary in the detection and investigation of drug and human trafficking and money laundering. Moreover, historical data are necessary to test new pre-determined criteria and ensure that they meet the requirements laid down in the Directive.

The data subjects concerned and categories of data processed

Under the PNR Directive, the processing of PNR data concerns all passengers on inbound and outbound extra-EU flights. Such broad coverage is necessary to achieve the Directive's intended objectives. In this respect, the Court in Opinion 1/15 acknowledged that 'the exclusion of certain categories of persons, or areas of origin, would be such as to hinder the achievement of the objective of automated processing of PNR data', that is to say, the prior identification of persons who may represent a risk to public security 'among all air

passengers'.[51] Furthermore, while it is undoubtedly the case that PNR data may 'reveal very specific information' on a person's privacy, where relevant, as acknowledged by the Court of Justice 'the nature of that information is limited to certain aspects of private life",[52] in particular the aspects relating to air travel.

As to the data processed, it should be recalled that PNR data are collected initially by the airlines for their commercial use. As stated in its Recital (8), the Directive does not impose an obligation to collect or retain additional data, nor does it oblige passengers to submit data beyond those already provided to air carriers. As the data collected differ on each occasion, the level of intrusion into the privacy of individuals also varies and should not be equated in all cases with the maximum level that is theoretically possible under the Directive. The collection of data by air carriers is necessary not only for the performance of the transport contract, but also to satisfy the specific needs or expectations of passengers. Therefore, in drawing on the data collected by carriers for commercial purposes, the PNR Directive is less intrusive than a measure which would require passengers to supply all the data contained in its Annex I.

In line with clarity and precision requirements, the categories in Annex I reflect internationally agreed standards, in particular at ICAO level. While some of these categories are similar to the ones in the draft EU-Canada PNR agreement of which the Court criticised the lack of precision, they are overall drafted in a more precise manner (see e.g. headings 5 and 8 of Annex I).

In practice, Member States have confirmed that the possibility to collect such categories of PNR data – to the extent that the various data elements have been provided by the passenger - is necessary for the implementation of an effective and proportionate PNR system. As already noted, information on payment methods, baggage, travel itineraries and travel agencies can be the only means to identify potential perpetrators of criminal and terrorist acts through comparisons against predetermined criteria. The same applies to other categories such as seat information, date of booking, split/divided PNR information, ticketing field information, code share information and data concerning minors in the general remarks section. Other data elements, such as contact information, frequent traveller data or API, allow the authorities to verify the accuracy of PNR data and ensure that the system works in a targeted manner so that only those passengers who are genuinely suspicious are identified. In sum, the categories

[51] Point 187 of the Opinion.
[52] Point 150 of the Opinion.

referred to in Annex I to the Directive comprise types of data which are strictly necessary to achieve the objectives pursued.

Additional safeguards surrounding the processing of PNR data

The PNR Directive contains strict safeguards to further limit the degree of interference to the absolute minimum and ensure the proportionality of the methods of processing available to national authorities. The analysis of the national transposition measures indicate that, in general, these safeguards have been implemented in a compliant and effective manner by the Member States.

As already indicated, PNR data can only be processed for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, as defined by the Directive. This purpose limitation determines how the automated processing of passengers' data prior to their arrival or departure is carried out. The data can be compared only against databases used to combat terrorist offences and serious crimes, including databases on persons or objects sought or under alert. Such databases contain data of persons wanted by national law enforcement authorities in relation with serious and dangerous offences. Even though PNR data of all passengers are compared against such databases, including the data of bona fide passengers, such comparison does not generate a match for the vast majority of passengers, who are not involved in criminal or terrorist activities. As a result, their data are not further accessed.

Importantly, the PNR Directive strictly prohibits the processing of sensitive data.[53] This constitutes an important difference with regard to the pre-existing draft EU-Canada PNR agreement, as explicitly acknowledged by the Court of Justice in Opinion 1/15.[54] The more intimate part of private life therefore remains fully protected by the processing operations provided for in the PNR Directive. Under the Directive, the information revealed by the processing of PNR data is in fact limited to the circumstances of the passenger's travel and would be established on the basis of data provided by the passengers themselves.

The processing against pre-determined criteria is also limited by important safeguards. The criteria used must be targeted, proportionate and specific to the aim pursued and are subject to regular review. They cannot be based on sensitive data and the assessment cannot be carried

53 See Annex I of the Directive and Article 6.4.
54 See Articles 6.4, 7.6 and 13.4 of the PNR Directive and point 166 of the Opinion.

out in a discriminatory manner. This limits the risk that discriminatory profiling will be carried out by the authorities.

Moreover, in practical terms, PNR data are not used to establish an individual profile of all passengers, but to assess risk and establish anonymous scenarios. Such 'abstract profiles' may consist, for example, of travel itineraries and behaviours associated with the preparation or commission of crimes such as suspicious payment methods or booking patterns (in cash, last-minute bookings, use of specific booking intermediaries).

Any results obtained through automated processing must also be verified by non-automated means. This obligation ensures the elimination of the so-called 'false positive matches', i.e. situations in which a comparison of a passenger's data with a database or watch list generates a match which is not confirmed by further processing, e.g. when a person included in a database has the same name as the passenger, but is not the same person.

The safeguards surrounding the automated processing of PNR data guarantee that only the data of a very limited number of passengers will be transferred to competent authorities for further processing. Indeed, the statistics gathered by the Commission for 2019 indicate that 0.59% of all passengers whose data have been collected have been identified through automated processing as requiring further examination. An even smaller fraction of 0.11% was transmitted to competent authorities.[55] This means that, overall, PNR systems deliver targeted results which limit the degree of interference with the rights to privacy and the protection of personal data of the vast majority of bona fide travellers.

With regard to the processing of historical PNR data, two main safeguards have been put in place to ensure the proportionality of data processing. Firstly, after passengers' arrival or departure, their data can only be processed to respond to a duly reasoned request from the competent authorities. The requesting authority must provide sufficient grounds to justify that the data are necessary for the prevention, detection, investigation and prosecution of terrorist offences or serious crime. Each request must be assessed by the Passenger Information Unit on a case-by-case basis. Secondly, after six months, all passengers' data are depersonalised. All the elements, such as name or contact details, which enable the identification of the passenger, become invisible to the user. The data can be unmasked (i.e. these elements can be made visible), but only with approval of a judicial or other authority and if necessary to respond to a duly reasoned request from competent authorities. If the authorising authority is

[55] For 2018 the rate was at 0.25% for matches resulting from automated processing and 0.04% for hits confirmed after an individual review.

not a judicial authority, the disclosure of the full PNR data are subject to informing the Data Protection Officer and to an ex-post review by that Data Protection Officer.

Case studies illustrating the different means of processing PNR data:

A fugitive convicted to a six-year prison sentence for drug-related offences was wanted by the authorities. The processing of PNR data, received by the Passenger Information Unit at least 24 hours before the flight departure, allowed to notify the relevant authority well in advance and to prepare for action before the arrival of the airplane, coming from a non-EU country. The individual was arrested immediately after arrival and brought before a judge.

In another example, four individuals belonging to an organised crime group were wanted for kidnapping and attempted murder of an adolescent, aged 17. The video recording of this violent assault was widely shared on social media and caused widespread shock. The processing of PNR data established that one of the suspects was on a plane arriving from Asia. The man was arrested upon arrival. The investigators also found his car in the airport carpark. The analysis of the car's navigation system led to the discovery of the victim's body, abandoned 200 km away from the crime scene.

A Passenger Information Unit transferred information regarding suspicious travel patterns of persons linked to a specific company to a unit dealing with organised crime. On the basis of the information provided by the Passenger Information Unit, the organised crime unit launched an investigation into the activities of individuals previously unknown to law enforcement authorities. The investigation revealed their involvement in money laundering and other international economic crimes.

In one Member State, convicted sex offenders must notify their intention to travel abroad and may be refused authorisation if the destination is considered to present a risk. A disproportionate number of convicted offenders declared travels to Dubai. However, the processing of PNR data showed that these offenders booked further flights to destinations to which travel would not have been authorised. The processing also enabled the authorities to establish that all the bookings were made by the same employee of a travel agency. Without PNR processing, the authorities would have not been able to establish the link between the passengers and the travel agency and would not have known about their final destination.

In another case, PNR processing revealed that three children were travelling unaccompanied outside Europe. There was no information on who should receive them upon their arrival. The authorities of the country of arrival were alerted and carried out a control on the person

waiting for the children, who turned out to be a convicted sex offender. Without the processing of PNR data, it would have not been possible to know that the children were travelling unaccompanied and no additional controls would have been carried out.

The use of pre-determined criteria indicated that an individual might be potentially travelling to a terrorist training camp. An analysis on the persons' travel history revealed that the person had travelled to this destination many times before, while trying to conceal the final destination. The individual's involvement in a violent extremist organisation, responsible for several terrorist attacks, was later confirmed.

5.2. The length of the data retention period

Article 12.1 of the PNR Directive requires the Member States to retain the PNR data transferred by air carriers for five years. This retention period is justified by objective considerations linked to the way PNR systems operate and the nature and length of criminal investigations.

Firstly, the need to retain data for five years stems from the nature of PNR as an analytical tool aimed not only at identifying known threats but also at uncovering unknown risks. Travel arrangements recorded as PNR data are used to identify specific behavioural patterns (that is, instances of repeated behaviour) and make associations between known and unknown people. By definition, the identification of such patterns and associations calls for the possibility of long-term analysis. In turn, this analysis requires that a sufficient pool of data is available to the Passenger Information Unit for such a relatively long period.

In particular, the pre-determined criteria used in the automated processing of PNR data are reprogrammed and refined regularly in order to ensure that they are targeted, proportionate and specific and avoid false positive results, i.e. the wrong reporting of persons who do not present a risk. These false positives constitute a greater interference with fundamental rights than the mere storage of PNR in the Passenger Information Unit database, as such data are never brought to the attention of the Passenger Information Unit staff.

To upgrade the pre-determined criteria, the software used for PNR processing must be capable of distinguishing 'normal' behaviours from those that can be objectively assumed to indicate a risk. This distinction must be based on reliable benchmarks, which can only be established if the IT system is supported by a database that represents the whole passenger population and its macro trends over time. Notably, some threats are rare, others are of a seasonal nature, so they would be impossible to detect if historical data were not retained for a

long period of time. Therefore, the generalised retention of passenger data is necessary for the Passenger Information Unit to assess passengers prior to their arrival or departure in an effective and proportionate manner.

Secondly, the retention of PNR data for five years is needed to ensure the effective investigation and prosecution of terrorist offences and serious crime. Investigating and prosecuting such offences usually involves months and, often, years of work. In many cases, the investigation concerns acts committed some time beforehand. Even if the arrest shortly follows the criminal act, it may be revealed that the same person might have been involved in other criminal activities and/or cooperate in their commission with other persons. Importantly, a passenger may be identified as posing a risk only at a later stage, and not in the automated assessment carried out by the Passenger Information Unit prior to arrival or departure. For example, a connection with a terrorist or criminal organisation may only be detected when more information becomes available, as an investigation progresses or following the commission of crime or a terrorist attack.

In this vein, Member States have confirmed that the five-year retention period is necessary from an operational point of view. The availability of historical data ensures that when an individual is accused of having committed a serious crime or being involved in terrorist activities, it is possible to review the person's travel history and see who they have travelled with, identifying potential accomplices or other members of a crime group, as well as potential victims. National authorities have also reported that, in some cases, the analysis of historical PNR data has been the only tool available to establish or prove the links between the persons involved in the commission of an offence. Historical data can also be used to verify the alibi of a suspect or to establish in an unquestionable manner that a lead is not valid or reliable enough to continue to be pursued.

In addition, the safeguards provided in the PNR Directive concerning access by the competent authorities to the data stored by the Passenger Information Unit and in relation to the depersonalisation and unmasking of data aim to prevent abuses. In particular, historical data can only be accessed on a case-by-case basis, in response to a duly reasoned request from competent authorities. Such a request must be based on sufficient grounds for the competent authorities to process PNR data, in relation to a specific case, for the purposes of the Directive. Following depersonalisation, the full disclosure ('unmasking') of PNR data requires an authorisation from a judicial or other authority, which must be preceded by the

analysis of necessity of such a disclosure for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

Finally, in respect of the time limits for retaining the PNR data to be transmitted to Canada, considered by the Court of Justice in Opinion 1/15, it is important to note that the performance of border controls is not a purpose of the PNR Directive, which clearly seeks the objective of ensuring security in the Union and its area without internal borders, where the Member States share responsibility for ensuring public security. In addition, unlike the draft agreement with Canada, the Directive does not concern data transfers to a third country, but the collection of passenger data from and to the EU by the Member States. In practical terms, for passengers returning to the Union to reside there it may be impossible to determine the timing of the erasure of the data given that they will not depart from the territory of the Member States. As a result, it can be concluded that the rule of erasure on exit laid down in Opinion 1/15 does not correspond to the objectives of the Directive and to the situation it seeks to regulate.

In a similar vein, the nature of the PNR Directive as secondary law means that its application is surrounded by the additional guarantees intrinsic to the *acquis*, and thus takes place under the control of the national courts of the Member States and, in the final instance, of the Court of Justice. Furthermore, the national laws implementing the Law Enforcement Directive also apply to the processing of data provided for in the PNR Directive, including any subsequent processing by competent authorities. Such considerations cannot be applied in the context of an international agreement involving the transfer of personal data outside the EU.

Case studies illustrating the use of historical data:

The police in a Member State was engaged in an ongoing investigation wherein it was gathering evidence to prosecute a suspect accused of human trafficking, in the context of the activities of an organised crime group. To link the suspect with the victims, information about a flight made in 2015 was necessary. As the Passenger Information Unit of that Member State had been established after this date, it made a request to the Passenger Information Unit which was operating in the destination of the relevant flight. The requested Passenger Information Unit was able to transmit flight information that linked the suspect with the victims (all passengers had been booked under one PNR) and provided the necessary evidence against the suspect.

In another case, two persons were arrested and charged with drug trafficking. Despite the fact that the arrest took place in a public place, when the defendants were exchanging drugs

and money, they both denied knowing each other when interrogated. However, the analysis of PNR data established that they had travelled together 20 times during a period of 2 years. They had not only booked the same flights, but also travelled next to one another.

A Passenger Information Unit was requested to provide travel information related to a person suspected to have been involved in ISIS activities in Syria before being arrested in another Member State. Intelligence available on the suspect pointed to a rich travel history around Europe. The analysis of PNR data allowed to trace back the movements of this individual between several Member States and to identify potential co-travellers. This information played a crucial role in this specific investigation and provided valuable insights into new travel patterns of ISIS members returning to Europe.

An individual had been wanted by law enforcement in relation to serious drug offences for more than 10 years. Intelligence indicated that the individual was a frequent traveller to other European countries, but no details of the person's travel history could be identified. Communications data analysis of a telephone number attributed to the individual revealed when their phone was in certain countries. Analysis of passenger data for flights to and from those locations on specified days revealed a single otherwise unknown individual whose travel destination matched the location of the mobile telephone. Analysis of this individual's PNR revealed a previously unknown identity, email address and residential address. This intelligence-led investigative work led to the person's arrest. Without the use of historical PNR data, this arrest would have not been possible.

The use of pre-determined criteria, developed on the basis of historical data, enabled the arrest of a passenger upon the arrival from Airport X with 4kg of heroin. The previously unknown passenger's PNR contained data elements that corresponded to pre-determined criteria created after the arrest of other drug smugglers.

5.3. The effectiveness of exchange of information between the Member States

One of the key objectives of the PNR Directive is to lay the foundations of an EU PNR mechanism. The Directive does not foresee the creation of a centralised database. Each Member State is competent for the collection, processing and storage of PNR data from the flights arriving and departing from its territory. At the same time, the cooperation and exchange of PNR data between the Passenger Information Units is one of the most important elements of the Directive.

The regular meetings on the application of the PNR Directive, organised by the Commission, as well as the Informal Working Group on PNR, led by the Member States, have allowed for the creation of a 'EU PNR community', where national authorities can discuss, exchange ideas, share best practices and address the issues arising from the practical application of the Directive.

The PNR Directive sets out two options for data transfers between the Passenger Information Units. In the first scenario, a Passenger Information Unit may transfer PNR data on its own initiative, when it considers this is 'relevant and necessary' for the prevention, investigation and prosecution of terrorist offences and serious crime in another Member State (the so-called 'spontaneous transfers'). The second scenario envisages that a Passenger Information Unit transfers data in reply to a request received from the Passenger Information Unit of another Member State. Such a request should be justified and the reasons provided must be relevant for the prevention, investigation and prosecution of terrorist offences and serious crime. The Directive sets additional requirements for the transfer of data that had previously been depersonalised.

According to national authorities, the exchange of data between the Member States based on requests functions in an effective manner. The number of requests has grown consistently and national authorities consider the possibility to request data from another Passenger Information Unit as both very useful and practical. Member States have adopted certain practical tools that facilitate the exchange of PNR data between the Passenger Information Units. For example, a large majority of Member States use a common template to request data. This helps prevent the impact of possible divergences in the interpretation of the requirement to provide due reasons for each requests. The rate of refusals is low, with most Member States having refused to share data only sporadically or having responded positively to all requests. The delay in providing a reply varies from a few hours to a few days, depending on the availability of staff and other factors such as whether the data requested have already been depersonalised or the seriousness of the crime in question (e.g. some Passenger Information Units prioritise requests related to terrorist offences). In general, PNR practitioners do not consider the time necessary to receive the requested data as an obstacle to the efficient cooperation between the Passenger Information Units. Most Member States use the Europol Secure Information Exchange Network Application (SIENA) for their communications with the Passenger Information Units of other Member States and the experience has been overall positive, although minor technical and other issues have been encountered.

In terms of challenges, national authorities have pointed out to the increasing number of requests and the impact of the divergences in national regulations and practices on the cooperation between the Passenger Information Units. Some practitioners have expressed concerns that the rapidly growing number of requests received both from their own national competent authorities and the Passenger Information Units of other Member States might create an excessive workload for their Passenger Information Units and lead to longer delays in processing data. Of particular concern is the practice of sending broad and unspecified requests to many (or even all Passenger Information Units). Such requests, even if refused as not duly reasoned, create an additional burden for the Passenger Information Unit staff.[56]

National authorities have also pointed out to divergences in national legislation as affecting the cooperation between the Passenger Information Units. In particular, national authorities may be more or less strict in assessing if a request is duly reasoned. Some may be stricter in requiring the proof of a link between the request and their Member States, whereas others may be more flexible. The fact that the Passenger Information Units are embedded in different authorities in the Member States (Ministry of Interior, Border Guard, state security agency), and differ in terms of their competences and tasks, may also have an impact on their cooperation. The lack of harmonisation of national criminal laws leads to additional complexity in this respect. With regard to the serious crimes listed in the PNR Directive, the terminology, classification and applicable sanctions vary across the Member States, which may result in differences in the scope of application. Another problematic element is the lack of feedback – a Passenger Information Unit will not know why a particular request has been refused.

In contrast with the widespread use of request-based information exchanges, the possibility to transfer PNR data on the Passenger Information Unit's own initiative is much less prevalent. A significant number of Member State have never spontaneously transferred data to other Member States. Others use this possibility sporadically or have rather developed a practice of providing additional information in reply to a request. Importantly, Member States vary in their interpretation of the concept of 'relevant and necessary': some consider that hits

[56] As explained before, the PNR Directive does not foresee the creation of any shared database or other centralised component. Whereas most Member States agree that the indication of a clear link with the requested Member State should be a mandatory element of a duly reasoned request, in some instances it may be difficult to determine which Passenger Information Unit may have the relevant information (e.g. if it is not known where exactly the suspect has travelled). The PIU.net project, funded under the ISF-Police Union Actions, has explored the possibility of creating an application which would allow to identify the Passenger Information Unit(s) which are likely to have the relevant data before a request is sent. For further details see Section 3.1 above.

resulting from processing against watch lists and databases as an indication of relevance and necessity, whereas others rely on a case-by-case individual assessment of relevance and necessity by Passenger Information Unit staff.

In conclusion, national authorities have identified the broad and relatively unclear formulation of the Directive's provision on spontaneous transfers as a reason for divergences in its interpretation and a certain reticence in its application. Others have also indicated that the Passenger Information Units have no human and technical capacity to conduct assessments targeted at the needs of other Member States and to engage in proactive transfers of data. Nevertheless, some practitioners have confirmed the usefulness of information received spontaneously (without a request) from another Passenger Information Unit.

Member States have not yet made use of the request possibilities linked to emergency situations and specific and actual threats, provided for in Articles 9.3 and 9.4.

5.4. The quality of the assessments including with regard to the statistical information gathered pursuant to Article 20

The analysis presented above was informed by quantitative and qualitative information gathered by the Commission in the preparation of the review. The sources of evidence used included Member States' statistical submissions and brief case studies illustrating the use of PNR data, discussions in dedicated workshops and other meetings on the implementation of the PNR Directive as well as field visits to the Passenger Information Units of specific Member States. Throughout the review process, national authorities and other stakeholders involved in the practical application of the Directive were open to share information and experiences with the Commission.[57]

In this regard, it must be noted that Article 20 of the PNR Directive requires Member States to collect, as a minimum, statistical information on the total number of passengers whose PNR data have been collected and exchanged, and the number of passengers identified for further examination.[58] As indicated above, the analysis of this information leads to the conclusion that only the data of a very small fraction of passengers are transferred to competent authorities for further examination. Thus, the statistics available indicate that, overall, PNR systems are working in line with the objective of identifying high risk passengers without impinging on bona fide travel flows.

[57] More information on the methodology and sources of information can be found in the Introduction.
[58] Article 20(2).

It should be noted that the statistics provided to the Commission are not fully standardised and therefore not amenable to hard quantitative analysis. This issue is compounded by the relatively early stage of development of most national PNR systems and the fact that the coverage of data collection still varies across the Member States. The Commission has mitigated these difficulties by collecting various types of evidence, as discussed above, to establish a solid evidence base for the review. Importantly, in most investigations PNR data constitutes a tool, or a piece of evidence, among others, and it is thus often not possible to isolate the results attributable specifically to the use of PNR alone, or to draw conclusions on its effectiveness based solely on quantitative assessments. For this reason, a combination of quantitative and qualitative sources appears to be better suited for this type of analysis. The Commission will also continue working closely with the Member States to improve the quality of the statistical information collected under the Directive.

5.5. Feedback from Member States on the possible extension of the obligations and the use of data under the PNR Directive

Intra-EU flights

Under the PNR Directive, Member States are allowed but not obliged to collect PNR data on intra-EU flights, in which case they have to inform the Commission (Article 2). However, because of the current security situation in Europe, on 18 April 2016 Member States declared in a statement that they intended to make full use of the possibility provided for in the Directive of requiring PNR on intra-EU flights.[59] All Member States but one have notified the Commission on the collection of PNR data in intra-EU flights under Article 2. Nevertheless, any such extension of the scope of the Directive must be subject to an impact assessment, including an assessment of its necessity and proportionality.

The collection of PNR data for intra-EU (and in particular intra-Schengen) flights is an important tool for law enforcement authorities to track the movements of known suspects and to identify suspicious travel patterns of unknown individuals who may be involved in criminal/terrorist activities when they travel within the Schengen zone. Some national authorities have reported, based on their operational experience, that the processing of PNR data for intra-EU flights produces significant number of matches, in some cases higher than for extra-EU flights.

Case studies illustrating the use of PNR data collected on intra-EU flights:

[59] Statement by the Council, 7829/16.

A third country national residing in one Member State was prohibited from entering the territory of another Member State because of links with a terrorist organisation. It was only thanks to the processing of PNR data that the individual's presence on a plane was discovered by the authorities. The person was intercepted immediately after arrival and sent back on the same day.

Based on the information provided by the Passenger Information Unit of Member State A, related to a match obtained by comparing PNR data with the SIS, the Border Police of Member State B was alerted while a person of interest was travelling from Member State A and the individual was arrested in compliance with an European Arrest Warrant issued by Member State C. As this was an intra-EU flight, passengers were not subject to border controls. Only the collection of PNR data made it possible to identify the target and conduct the arrest.

Non-carrier economic operators

The Directive does not require travel agencies and tour operators (the 'non-carrier economic operators') to send PNR data but does not prohibit Member States to also collect PNR from these entities under their national law, if such measures are compatible with the EU law. In a few Member States, national legislation provides for a legal basis for such collection, but it is not implemented in any of them.[60]

Tour operators and travel agencies provide travel-related services, including the booking of both regular and charter flights. To make a booking they collect passengers' information, which may include, in addition to name and surname, the contact and payment details. However, only very limited information is further provided to the airlines in order to finalise the reservation. In most cases, only name, surname and information on the passenger being an infant or child is shared with the airlines. In addition, the exact data elements transferred to airlines, as well as the timing and the technical modalities of the transfer, differ depending on the carrier.

Travel agencies and tour operators have reported that, due to business considerations, they are unwilling to transfer to airlines (or to other tour operators) data elements other than those that they consider strictly necessary. Their main concern is that passengers' contact details may be used by airlines to approach them directly to propose services. As a result, for reservations

[60] The Directive does not prevent Member States from extending the obligation to transfer PNR data to non-carrier economic operators (see Recital 33).

made by non-carrier economic operators, only very limited data elements are transmitted to the Passenger Information Units.

However, the contact details and payment information may be very relevant for law enforcement authorities. For instance, the same email address or credit card may be used by members of a group involved in criminal or terrorist activities. The processing of such data may allow to identify the links between seemingly unrelated passengers and trace the movements of the members of the group. Given that, depending on the Member State, up to 50% of flight reservations may be made by travel agencies and tour operators, an important share of the data provided by passengers is not collected and processed by the Passenger Information Units, which creates an important security gap.

Importantly, the concerns of non-carrier economic operators that their competitors could use the data of customers for their own commercial purposes would not be relevant in case of data transfers to the Passenger Information Units. However, the extension of data collection to non-carrier economic operators will require a detailed analysis of the legal, financial and technical aspects stemming from such extension, like the lack of standardisation of data formats.

Other modes of transportation

The Directive does not exclude that Member States might provide, under their national law, also for the collection and processing of PNR from other transportation services providers, if this is compatible with Union law (Recital (33)). Any such extension of the scope must be subject to an impact assessment, including as to its proportionality and necessity. This possibility has been used so far only by a few Member States, which extended passenger data collection to other modes of transport, namely maritime, rail and road carriers.[61] These regulations are still at an early stage of implementation. However, a number of positive operational experiences have already been shared by the authorities using passenger data collected on these transportation modes.

Serious concerns have been raised by law enforcement experts with regard to the lack of collection of passengers' data from other modes of transportation. The phenomenon of 'broken travels', by which criminals divide their travel and use different modes of

[61] In Belgium, national law extends the collection of PNR data to international high-speed trains and the international bus sector; however, the implementation is at a very early stage. Estonia collects ferry passenger's data. French legislation foresees the collection of API and PNR for maritime transport. In Sweden, the Police and Customs have access to passengers' data from other modes of transportation, but the scope of the applicable legislation is more limited than the PNR Directive.

transportation to conceal their final destination,[62] is well known to law enforcement authorities. These have warned that the progressive deployment of PNR data collection in the air sector may bring about changes in travel patterns of persons involved in terrorism and serious crime, who may increasingly choose other modes of transportation.

At the same time, the collection of passenger data for other modes of transportation raises practical, technical and legal questions, including considerations on their impact on fundamental rights. Firstly, passenger data formats are not as standardised for other modes of transportation as the PNR for the air sector. In addition, rail and road transport present very different characteristics: a ticket can be bought at the very last moment (or even already on board) and in many cases is not nominal. The journey may have many stops before reaching the final destination, with passengers starting and finishing the journey at different moments.

The possibility of extending PNR collection to other modes of transportation was discussed within the Council Working Party on Information Exchange and Data Protection (DAPIX), under the Finish Presidency during the second semester of 2019. These discussions led to the adoption of Council conclusions of 2 December 2019 on 'Widening the scope of passenger name record (PNR) data legislation to transport forms other than air traffic'.[63] The conclusions note that some Member States have acknowledged the potential added value of extending PNR data collection to other transport modes for the fight against terrorist offences and serious crime, while also taking stock of the concerns voiced by some Member States regarding the legal, technical and financial challenges this could create, in particular with regard to fundamental rights and the principles of necessity and proportionality. The document recommends that a thorough assessment be carried out before any further decisions may be made in this regard.[64]

The use of PNR data to protect public health in case of a pandemic

A number of Member States have pointed out that PNR data could constitute a valuable tool to protect public health, in particular to prevent the spread of infectious diseases. On the latter, the seat information – which could allow the health authorities to identify passengers who had been in the proximity of a person who was subsequently diagnosed as with an infectious

62 Instead of taking a direct flight, a person may travel by plane to another destination and then continue by taking a train or ferry.

63 14746/19.

64 In particular, with regard to the maritime sector, the possible impact on the legal obligations arising from Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community (OJ L 188, 2.7.1998, p. 35) would need to be taken into account.

disease – could be important in case of epidemics. This issue has gained more prominence since the beginning of the COVID-19 pandemic in 2020, with more Member States indicating that there is a need to be able to use PNR data to tackle such health-related emergencies.

The PNR Directive currently only allows for the processing of PNR data in the fight against terrorism and serious crime, with no exceptions. By way of comparison, the EU PNR agreement with Australia does recognise that there may be exceptional circumstances where PNR can be processed to protect the vital interests of any individual, such as a risk of death or serious injury or a significant public health risk.[65] The Court of Justice, in its Opinion 1/15 on the draft EU-Canada PNR agreement, has also accepted the exceptional use of PNR for such purposes.[66]

6. KEY OPERATIONAL CHALLENGES

Based on the consultations with the Member States and other stakeholders, the key four challenges below were identified:

6.1. Reliability of PNR data

PNR data are generally provided by the passengers themselves. In accordance with Article 8 of the Directive, air carriers are obliged to transmit PNR data to the extent that they have already collected such data in the normal course of their business. Accordingly, air carriers are not obliged to ensure that the data transmitted to the authorities are complete, accurate and up-to-date. Under the PNR Directive, carriers can only be sanctioned for failing to transmit the PNR data they have or for not doing so in the right format (Article 14). National authorities have identified issues arising from the poor quality and incompleteness of PNR data as the main challenge preventing them from using PNR data to its full potential. However, air carriers argue that concepts such as 'quality' and 'completeness' should not be applicable to PNR given its declaratory and unverified nature.

When speaking of data quality, law enforcement authorities usually refer to issues such as spelling mistakes, data elements being misplaced in the PNR message (e.g. the email address is contained in the field for payment details) and the fact that in some cases abbreviations

[65] Article 3.4 of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, p. 4. See also Article 3 of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 5.

[66] Paragraph 179-180 of the Opinion. The GDPR also acknowledges that the processing of personal data may serve both important grounds of public interest and the vital interests of the data subject, in particular when used for monitoring epidemics and their spread, and contains provisions to this end.

such as Mr are attached to passengers' surnames, among others. These seemingly minor details may have a significant impact on the automated processing of PNR data: the data received by the Passenger Information Unit may be unreadable to the IT system or require additional maintenance and adaptations. At the same time, air carriers do not have any obligation to verify this kind of issues before transferring PNR data.

As regards completeness, air carriers have further underlined that the amount of data collected are determined by commercial considerations. The reservation data collected can be very limited, in some cases including only the name and the surname of the passenger, combined with the basic information about the flight (date, itinerary). In turn, national authorities point out that the lack of certain data allowing to confirm the passengers' identity impairs the efficient use of PNR data and constitutes a key challenge for the Passenger Information Unit staff in their daily work.

Notably, without the date of birth it may be impossible to confirm the identity of the person, particularly for passengers with common names. This may hinder the possibility to compare PNR data against certain databases relevant for the fight against terrorism and serious crime – including the SIS –[67] which require the use of more complete data for a person to carry out a meaningful search. For example, one Member State reported that a large majority of matches have to be discarded as the manual intervention needed to confirm the result of automated processing would be too cumbersome, and ultimately impossible, in the absence of additional elements necessary to confirm the identity of the passenger.

API data play a very important role in this regard. API data are basic information about passengers and crewmembers. It includes elements such as the name, date of birth, gender, citizenship, and travel document data (e.g. passport number). This information is usually available from the machine-readable zone of travel documents. Unlike PNR, API is generally not required for air carriers' commercial processes and would therefore only be collected by them if there is a legal requirement. For air carriers operating flights to the Member States, such a legal requirement arises from the Council Directive 2004/82/EC, also known as the 'API Directive', but only for passengers of flights arriving to a Member State from a third country. In contrast to the PNR Directive, the API Directive does allow for sanctions when carriers transmit incomplete or false data. If collected, API will constitute an element of the

[67] Additional details on this particular issue are provided in Section 6.4 below.

PNR data and will be transferred to the Passenger Information Unit – either together with PNR or separately, if the airline retains API by separate technical means.[68]

The availability of more data elements, and in particular the date of birth, enables the processing to be more targeted and specific. In particular, it reduces the number of false positive matches and makes the processing of PNR data less intrusive. This is because many of the marches that are currently being confirmed manually would not be generated in the first place, as the additional data elements collected would already exclude them. However, as indicated above, API is not collected on all flights and is generally lacking for intra-EU journeys (even though carriers are required to transfer PNR on those flights in most of the Member States). Some carriers have made the conscious commercial choice to request additional data from passengers, and incentivise them to ensure that the data provided are accurate (e.g. by imposing extra fees in case of erroneous encoding). National authorities underline that in these cases the reliability of PNR data increases dramatically.

Law enforcement practitioners in the Member States also stress that the best operational results are often achieved by the joint processing of the more reliable API data,[69] which enables the confirmation of the identity of passengers, together with richer PNR, which reveals important information about passengers' travel behaviour. As a result, most PNR practitioners advocate for the need to expand the collection of API to intra-EU flights, as a measure to boost the reliability of the PNR data set. As an alternative, some national authorities have suggested that the mandatory collection of the date of birth by air carriers should be envisaged. However, the possible extension of such obligation to intra-EU flights should be preceded by an impact assessment, including from the point of view of its necessity and proportionality. The Commission is currently evaluating the API Directive. Following the completion of this assessment, the Commission will decide on the way forward and steps needed to be taken to revise the Directive.

6.2. Challenges identified by the air industry

Air carriers and their associations have identified a number of difficulties in the implementation of the PNR Directive.

---

[68] This is the case, for example, when air carriers have segregated systems and they store PNR in their reservation system and API in their check in system.

[69] API data are collected at the moment of check-in. In case of online check in, API data will also be declaratory. Nevertheless, given that most passengers introduce correct data, this information is still useful.

Occasionally, airlines have reported being faced with requests going beyond the requirements of the Directive. For instance, in relation to a few Member States, airlines described being 'strongly encouraged' by the authorities to use one specific communication protocol to transmit PNR, in contradiction with the Directive, which allows each air carrier to choose.[70] In some cases, depending on the system provider chosen by the Passenger Information Unit, airlines have been requested by the service providers to bear additional costs.

In addition, the higher number of data pushes required by some Member States have been said to create an operational and cost burden for airlines. Furthermore, some authorities allegedly still lack a good understanding of the different sets of passenger data (i.e. API and PNR data), their nature and how they are operationally and technically handled by airlines.[71] Lastly, the representatives of the air industry criticise the lack of flexibility on the part of some national authorities, which allegedly have an imperfect understanding of the complexities of the connectivity process and the difficulties faced by carriers to accelerate it.[72]

Business aviation operators have signalled challenges linked to the particular characteristics of their sector and its operating modes. Some operators, especially the smaller ones, do not use reservation systems, flights are often booked at the very last moment and the itinerary may be even changed after take-off. The requirements imposed on business aviation vary depending on the Member State, which combined with the fact that many companies change their destinations on an *ad hoc* basis, makes it very difficult to ensure compliance and avoid penalties.[73]

All consulted industry stakeholders would welcome the setting up of a unique focal point operating as a single window for all categories of passenger data collected.

6.3. Scope/restrictive purpose limitation

As noted above, PNR data can be used only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and those serious crimes listed in Annex II to the PNR Directive that meet the punishment threshold specified in Article 3.9.

---

70 From the list of accepted protocols listed in Implementing Decision 2017/759.

71 This problem was also highlighted in the presentation of the Croatian Airlines, held in the framework of the Croatian Presidency, during a session of the Council Working Party on JHA Information Exchange (IXIM) on 3 June 2020.

72 This problem was exacerbated by the fact that many Passenger Information Units have started the connectivity process more or less at the same time.

73 Business aviation is included in the scope of the PNR Directive, to the extent that they collect PNR data. In practice, currently only a few Member States collect passenger data from business aviation.

Members States have reported that the Directive's purpose limitation does not always correspond with the important operational needs and challenges encountered by law enforcement authorities in their daily work. In particular, the limited scope of the Directive makes it difficult to cover certain criminal activities that, taken in isolation, may appear to be minor but in reality are linked to serious organised crime (e.g. pickpocketing networks in which there may also be an element of human trafficking). Furthermore, the fact that law enforcement officers should disregard certain hits as beyond the scope of the Directive also raises ethical concerns, given their duty to act when they come across an offence.

Member States have also pointed out that PNR data could play a vital role to achieve certain important objectives that are currently not covered by the Directive. In particular, PNR could constitute a valuable tool to track missing persons (including minors) or for the protection of public health. The scope of the PNR Directive is also narrower than of other EU instruments relevant to law enforcement cooperation, such as the European Arrest Warrant (EAW)[74] or the SIS.[75] For example, the EAW applies to all types of criminal offences and may be issued by a national judicial authority if the sought after person is accused of an offence for which the maximum penalty is at least one year of prison or the sought person has been sentenced to a prison term of at least four months.[76] For a list of thirty-two serious offences punishable by deprivation of liberty for at least three years, the surrender of the person does not require the verification of the double criminality of the act.[77] This list largely coincides with the list set out in Annex II of the PNR Directive, but is not exactly the same. Given that the SIS includes persons for whom an EAW has been issued among its alert categories,[78] these differences in scope may lead to PNR-SIS data resulting in matches for offences that fall outside the scope of the PNR Directive.

As a result, some Member States consider the current limitations to be inconsistent with the overall rationale of the EU framework for law enforcement cooperation and have pointed to the necessity of extending the scope of the Directive. This could be achieved in particular by

---

74 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision OJ L 190, 18.7.2002, p. 1.

75 For a more detailed analysis of issues arising from comparisons of PNR data against SIS, see the next section.

76 Article 2.1 of the Council Framework Decision 2002/584/JHA.

77 Article 2.2 of the Council Framework Decision 2002/584/JHA.

78 Article 26 of Council Decision 2007/533/JHA.

adding more criminal offences to the list in Annex II (e.g. to make it coherent with the EAW).[79]

6.4. Cross-checks against the SIS and other instruments

According to Article 6.3(a) of the PNR Directive, when pre-screening passengers prior to their arrival or departure, the Passenger Information Unit may compare PNR data against databases relevant for the purposes of fighting terrorism and serious crime 'including databases on persons or objects sought or under alert'. The SIS, the most widely used and largest information sharing system for security and border management in Europe, is clearly one of such databases.

The purpose of the SIS is to ensure a high level of security within the area of freedom, security and justice of the EU. The system enables competent authorities, such as the police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects in order to locate them. Many of the SIS' alert categories – for example on persons wanted for arrest as well as on persons and objects for discreet or specific checks – relate, largely or partly, to terrorism and serious criminal activities.

Most Member States already check PNR data against the SIS and emphasise, in particular, the law enforcement value of performing such an assessment on intra-EU flights, where no passenger data were available prior to the implementation of the PNR Directive. However, a number of legal and practical challenges have prevented the Member States from making the most of PNR-SIS data comparisons.

A first challenge stems from the fact that the identity information available in the PNR is often limited. For instance, information on the passenger's date of birth is usually lacking in intra-Schengen flights where airlines are not required to collect API. This affects the ability of Member States to query PNR data against the SIS – as the date of birth is required to perform exact matches – and creates uncertainty as to whether any positive results obtained in the pre-screening process indeed concern a person subject to an alert in the SIS. The individual manual review provided for in Article 6.5 of the PNR Directive protects individuals against the adverse impact of potential 'false positives' but can also significantly increase the workload of the Passenger Information Units.

[79] Such extension of scope would require a thorough impact assessment, including as regards the fundamental rights implications.

Another important issue concerns the broader scope of the SIS, compared to the PNR Directive, combined with the lack of sufficient detail concerning the type of offence underpinning a specific SIS alert. This raises the risk of the Passenger Information Unit obtaining matches that are not 'PNR-relevant' when performing database checks. Again, the manual review process, while offering the opportunity to dismiss any non-PNR related matches, is time and resource-intensive. Ignoring potential hits also raises complex legal questions, as the authorities usually have the duty to act when confronted with a possible criminal offence, irrespective of whether this fits the strict purpose limitation requirements of the PNR Directive. In practical terms, Member States have tackled these challenges in different ways. Some of them refrain from comparing PNR data against the SIS and limit such comparisons to national law enforcement repositories and pre-determined criteria. Others run PNR data queries only against specific SIS alerts, notably those under Articles 26 and Article 36.2 and 36.3 of Council Decision 2007/533/JHA.[80] While these approaches help limit the number of 'false positives'/ non-PNR related matches, they may also lead the authorities to miss potentially relevant information. For this reason, other Member States compare PNR data against all alert categories and rely on the manual validation step to filter out matches that do not specifically relate to the purposes of the PNR Directive, which in turn leads to the aforementioned efficiency issues, and raises questions as to whether these broad comparisons are fully aligned with the Directive's strict purpose limitation.

In the future, new challenges may emerge from the interaction between PNR and other instruments in the travel intelligence landscape, such as the European Travel Information and Authorisation System (ETIAS) and the Entry/Exit System (EES). Aspects that will warrant further examination concern, for example, the relationship between the Passenger Information Units and the ETIAS National Units in the Member States, and the way to ensure that all available travel information (in particular API, PNR and ETIAS related) is used in the most effective manner.

6.5. Requests from third countries

More and more third countries are asking air carriers operating to or from the EU to transmit PNR data, while currently a limited number of PNR agreements is in force or being negotiated between the EU and non-EU countries.

[80] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p. 63.

This gap between the number of countries demanding PNR data on EU flights and the number of countries which are effectively able to get such data from the EU is likely to increase in view of UN Security Council Resolution 2396 (2017) and the new ICAO standards, which make the development of PNR systems mandatory.

Now that Member States have started asking for PNR data from third countries under the EU PNR system, the frequency of requests for PNR data from the EU have intensified. In particular, several EU Member States have reported that specific non-EU countries have reacted to the refusal of EU airlines to transfer data by threatening and applying retaliatory measures, instructing their national carriers to stop PNR data transfers to the EU Member States. This is detrimental to the implementation of the PNR Directive and the overall EU PNR architecture and creates security gaps. The Commission is in contact with those third countries to inform them about the possibilities of carrying such transfers in accordance with the EU applicable legal framework. In that context, the Council has recently authorised the opening of negotiations for the conclusion of a PNR agreement with Japan.

The current situation also raises concerns for EU air carriers, who may be faced with a conflict of laws situation. On the one hand, a transfer of data would amount to a violation of EU data protection laws, on the other the refusal to comply with the laws of the country of destination may entail sanctions, such as heavy fines. To avoid that air carriers are faced with such conflict of law situations preventing them from transferring PNR data to and from the Member States, ways to allow the transfer of PNR data to third countries, in compliance with EU law requirements, will need to continue to be addressed in the context of the Commission's external PNR policy.[81]

[81] Currently laid down in the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final.