

# PNR ACT REVIEW

OCTOBER 2021



## Carried-out by:



UNIVERSITY OF AMSTERDAM  
Institute for Information Law

Dr. Kristina Irion & Romy van Es, LL.M.  
Institute for Information Law (IViR), University  
of Amsterdam  
<https://www.ivir.nl/>

it's public

Kees van der Meeren, Msc &  
Daphne Dijkman, MA LL.M.  
It's Public, Amsterdam  
[www.itspublic.nl](http://www.itspublic.nl)

## Commissioned by:



Wetenschappelijk Onderzoek- en  
Documentatiecentrum

## Summary

On 18 June 2019, the Dutch Act on the Use of Passenger Data to Combat Terrorist and Serious Crimes (PNR Act) entered into force.<sup>1</sup> This Act requires airlines to provide passenger data from every flight departing or arriving in the Netherlands to the Passenger Information Unit Netherlands (Pi-NL). Under that law, Pi-NL may process passenger data collected only for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. With the adoption of the PNR Act, the Dutch legislator is fulfilling its duty to implement EU Directive 2016/681 (PNR Directive).<sup>2</sup>

The PNR Directive creates an EU legal framework for the collection and use of personal data of passengers on flights to or from third countries. The PNR Directive leaves it to the discretion of the Member States whether to apply it to flights within the European Union (EU). If a Member State makes use of this option, all the provisions of the PNR Directive apply to these intra-EU flights as well. The Dutch legislator has also included intra-EU flights within the scope of the PNR Act.

The legal framework for the collection and use of passenger data introduced by the PNR Directive is subject to debate as it interferes with the fundamental rights of air passengers guaranteed in Articles 7 and 8 of the EU Charter. In the meantime, a number of court cases have been filed, requesting the Court of Justice of the European Union to rule on the legality of the PNR Directive in light of the Charter of Fundamental Rights of the European Union. A judgment from the Court is expected in the first half of 2022.

This research fulfils the obligation in Article 25 of the PNR Act that, two years after the entry into force of the Act, a review should be conducted of its effectiveness and impact in practice. This review also focuses on compliance with privacy safeguards and on the processing of passenger data from intra-EU flights. Article 25a of the PNR Act contains a sunset clause for the processing of data relating to intra-EU flights. Article 25a will enter into force three years after the entry into force of the PNR Act, unless an executive decree provides for its repeal.

The period covered by this review is from the Act's entry into force on 18 June 2019 to 5 July 2021.

---

<sup>1</sup> Act of 5 June 2019, laying down rules to implement 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 (OJEU 2016, L 119) (Act on the use of passenger data to combat terrorist offences and serious crime), *Stb.* 2019, p.205.

<sup>2</sup> Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. OJ L 119, 4.5.2016, p. 132–149.

## The use of passenger data under the PNR Act

In the Netherlands it has been decided that airlines shall provide passenger data to the Pi-NL at three points in time: 48 hours before departure, 24 hours before departure, and after the aircraft doors have been closed (0 hours). This passenger data includes reservation and check-in data and contains information on, e.g., reserved and previously travelled itineraries, co-passengers, baggage, contact and payment information. Under the PNR Act, passenger data can then be used to prevent, detect, investigate and prosecute terrorist offences and serious crime.

The Pi-NL is a specialised unit with its own statutory duties and powers to collect, store and process airline passenger data. Meeting the legal requirements, the Pi-NL is authorised to:

- compare passenger data against databases and pre-determined risk criteria prior to arrival in, or scheduled departure from, the Netherlands;
- provide passenger data or the result of the processing of such data to the national competent authorities and to Passenger Information Units (PIUs) of other Member States, Europol and authorities of third countries; and
- analyse passenger data for the purpose of updating or creating new risk criteria to be used to identify any persons who may be involved in a terrorist offence or serious crime.

The Pi-NL shall ensure that passenger data is retained for a period of five years after receipt and deleted after this period, and that passenger data shall be depersonalised six months after receipt.

The flowchart below (Figure 1) illustrates what happens to passenger data within the scope of the PNR law.

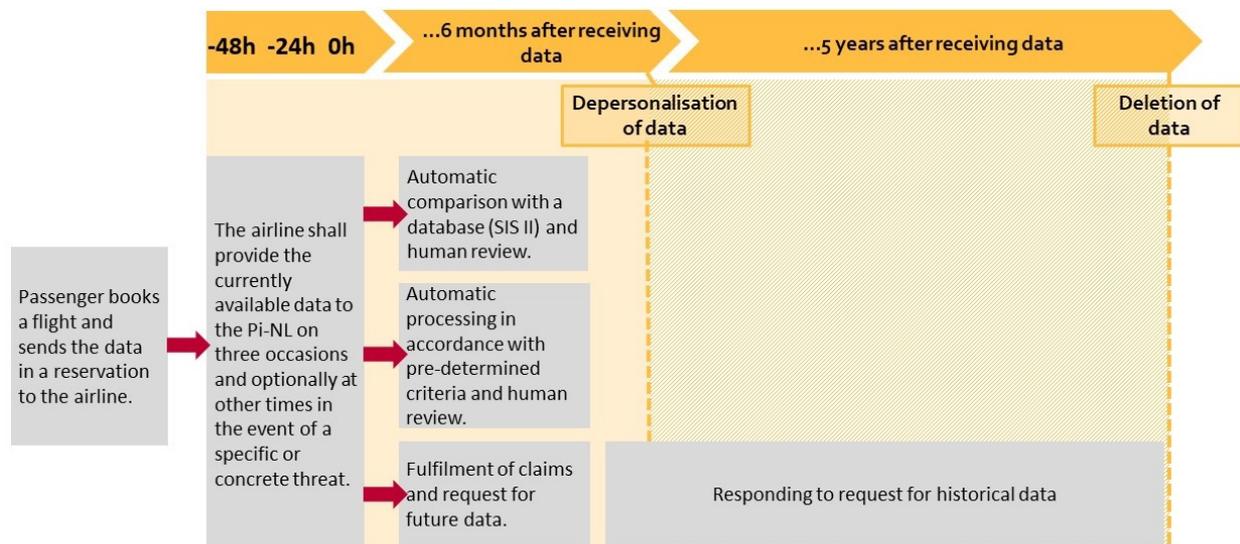


Figure 1. Flowchart passenger data processing by Pi-NL.

## Research questions and approach

The study 'PNR Act Review' seeks to answer the following **main question**:

***What is the use, effectiveness and impact of the PNR Act in practice since its entry into force on 18 June 2019?***

To answer this question, a number of **sub-questions** have been formulated:

***Research question 1:*** *What is the use of the PNR Act in practice since its entry into force on 18 June 2019 in quantitative terms (information exchanged under Article 9a to Article 16 of the PNR Act), broken down as far as possible by intra-EU and extra-EU, by inbound and outbound flights and associated passenger data, and by querying/receiving authority?*

***Research question 2:*** *What role did the exchanged passenger data play in the work of law enforcement agencies and what happened with it?*

***Research question 3:*** *To what extent are the applicable standards of privacy protection observed in the collection and processing of passenger data by the Pi-NL?*

***Research question 4:*** *Based on the application of the PNR law in practice to date, what can be said about the effectiveness, necessity and proportionality of including in the scope of the law the mandatory transfer of passenger data on intra-EU flights?*

The following **methods were used** to answer the research questions:

1. ***Document analysis.*** This involves mapping the legal framework and its implementation in practice based on various types of documents, including EU and Dutch legislation, policy and related documents, case law and academic sources.
2. ***Analysis of quantitative data.*** In order to map the use of the PNR Act, quantitative data has been collected and analysed. These data are entirely derived from the management systems of the Pi-NL.
3. ***Interviews with stakeholders.*** In order to gain insight into the use and effects of the PNR Act, 28 interviews were conducted with representatives of the various organisations involved. These included airlines, the Pi-NL, the Ministry of Justice and Security, competent authorities and civil society organisations.
4. ***Information visits to the Pi-NL and inspection of documents at the Ministry of Justice and Security.*** The researchers made two visits to the Pi-NL to learn about the practice, and one to the National Coordinator for Security and Counterterrorism for document access.

The research questions are answered as fully as possible using the methods described. However, not enough information is available to answer all questions. An evaluation with a practice focus of two years after the enactment of the PNR Act is very short to see results. Moreover, much of this period included the Covid-19 pandemic, which led to a huge drop in passenger air travel and, as a result, a sharp decline in passenger data collection, use, and demand by the Pi-NL.

## Findings of research questions

**Research question 1:** *What is the use of the PNR Act in practice since its entry into force on 18 June 2019 in quantitative terms (information exchanged under Article 9a to Article 16 of the PNR Act)?*

Since the PNR Act entered into force on 18 June 2019 to 1 January 2021, the Pi-NL has received data from 430,402 flights and from 61,431,852 passengers.<sup>3</sup> Of these passengers, approximately 65% flew intra-EU and 35% extra-EU. Currently 66 of the 81 airlines flying to the Netherlands provide passenger data to the Pi-NL. This represents 81% of the total number of passengers that have flown to or from the Netherlands.

Since the PNR Act entered into force until 1 January 2021, Dutch competent authorities have submitted 3,130 requests, and 435 information requests have been submitted by Europol, other PIUs, competent authorities of other EU Member States or authorities of third countries. Although the number of flights decreased due to the Covid-19 pandemic, the average number of requests per month in 2020 is above the level of 2019. The national police and the Royal Netherlands Marechaussee together account for 90% of the total number of requests submitted. The offences most commonly invoked in the requests are illicit trafficking in narcotics and psychotropic substances, laundering of proceeds of crime and counterfeiting, and participation in a criminal organisation.

Since the PNR Act entered into force until 1 January 2021, passenger data has been provided to Dutch competent authorities 20,034 times. The number of disclosures per month in 2020 is also higher on average than in 2019. In total, there were 12,393 disclosures in 2020 where passenger data of 6,216 passengers were shared with Dutch competent authorities. Most disclosures relate to illicit trafficking in narcotics and psychotropic substances, and laundering of proceeds of crime and counterfeiting of currency.

For approximately 0.025% of the passengers whose data has been shared with the Pi-NL, passenger data is also provided to competent authorities in the Netherlands. This is 25 out of every 100,000 passengers. This is the total number of times that passenger data has been shared. It is not known how many unique passengers' data have been shared.

In general, it can be said that the provision of passenger data under the PNR Act is increasing in a broad sense. From the above quantitative point of view, no statement can be made about the contribution of passenger data to the prevention, detection, investigation and prosecution of terrorist offences and serious crime. After all, it only concerns the demand for passenger data by the Dutch competent authorities.

**Research question 2:** *What role did the exchanged passenger data play in the work of law enforcement agencies and what happened with it?*

Although the input of passenger data provided for the purposes of the PNR Act is known, information on the resulting output is lacking. The use of the passenger data is not documented in the competent authorities' record-keeping systems. On the basis of the available information, it is hardly possible to determine what role these passenger data have played in criminal investigations. To date, there is no

---

<sup>3</sup> A passenger who flies several times is counted once for each flight. This means that a person flying a return flight whose data is collected on both the outbound and inbound flights counts as two passengers.

known decision by a criminal court in which passenger data that have been collected under the PNR Act were used as evidence.

To some extent, the demand for passenger data by the competent authorities is an indicator of its use, but it says nothing about its results and impact on the fight against terrorist and serious crime. However, on the basis of the interviews with the representatives of the competent authorities and Europol, it is possible to sketch the perceived usefulness of the passenger data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes. The competent authorities and Europol interviewed indicate that the PNR legislation adds value to their investigative practice.

The creation of the Pi-NL as a single information point for the collection, processing and transfer of the PNR data within the purpose of the PNR Act lowers the bar for the competent authorities to request such data. Before the PNR Act entered into force, it was possible to obtain passenger data from the airlines, but this was in most cases less efficient. At EU level, the PNR legal framework facilitates cooperation and exchange of passenger data.

Nevertheless, there are a number of obstacles to the use of passenger data by law enforcement agencies:

- a. **Data quality.** Passenger data is unverified data and therefore less reliable for determining the identity of a person.
- b. **Incompleteness.** Some data that are important for the work of the Pi-NL and the investigation services may be missing, such as the date of birth, from intra-EU flights. Data may also be incomplete, such as payment data.
- c. **Scope of the obligation to transfer.** It is not yet clear whether, under the PNR Act, airlines are also required to provide *Advanced Passenger Information (API)*<sup>4</sup> from the departure control system to the Pi-NL.

**Research question 3:** *To what extent are the applicable standards of privacy protection observed in the collection and processing of passenger data by the Pi-NL?*

Although the research question relates only to the Pi-NL, the controller should also be included in this assessment. After all, the Pi-NL implements the PNR Act under the responsibility of the Ministry of Justice and Security, which is also the controller responsible for the lawful processing of passenger data.

The essential privacy and personal data protection safeguards of the PNR Act and the Code of Criminal Procedure are applied, namely:

- a. the monitoring of the purpose limitation of the processing of passenger data by the Pi-NL on the basis of the PNR Act;
- b. the procedural protection by means of the authorisation of the public prosecutor in the case of disclosure on the basis of requests by competent authorities, Articles 126nd and 126ne of the Code of Criminal Procedure, and which concern passenger data older than six months; and

---

<sup>4</sup> Pursuant to Annex 2 No. 18 PNR Act, API data include: type, number, country of issue and date of validity of an identity document, nationality, surname, first name, sex, date of birth, air carrier, flight number, departure date, arrival date, airport of departure, airport of arrival, arrival time.

- c. the supervision by the Data Protection Officer in general and the ex-post control of the transmission of passenger data older than six months.

With regard to the processing of passenger data, the Pi-NL complies in general with the applicable standards of the PNR Act for the protection of privacy and personal data. The controller, the Ministry of Justice and Security, must take appropriate measures if there are indications that passenger data are not or cannot be processed in compliance with the law. Subsequently, the most important observations regarding compliance with the privacy safeguards of the PNR Act and applicable legislation are presented:

#### With regard to the collection of passenger data

- If modes of transport other than flights are stored by the Pi-NL, such as in certain cases train or bus transport booked as part of an air journey, this is not in accordance with the PNR Act.
- Under the PNR Act, the Pi-NL must not store special personal data that reveal a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. Since special personal data cannot be filtered out in a fully automated way, such data may still be amongst the retained passenger data.

#### With regard to the processing of passenger data

- The decision to designate the SIS II database does not specify the articles of the SIS II Regulation on the basis of which an automated comparison with passenger data is performed. This is because the purpose limitation of the PNR Act does not correspond to the scope of the SIS II database.
- At present, it is unclear what the objective standard is to ensure the proportionate and non-discriminatory application of a risk criteria set.
- Since the required human review following an automated positive match is not yet registered in the TRIP application, it cannot be demonstrated retrospectively either.

#### With regard to the transmission of passenger data

- A request for passenger data by Europol does not require prior authorisation by analogy with the Code of Criminal Procedure. Currently, the public prosecutor of the LIRC assesses the proportionality and subsidiarity of requests by Europol, but this is not foreseen by law.
- Instead of the SIENA system operated by Europol, the Data Protection Officer recommends that international transfer decisions are made within the TRIP application with the attendant legal safeguards.
- To give authorisation to the disclosure of historical passenger data older than six months that is otherwise depersonalised, the public prosecutor ticks a box in the request form. However, from the wording used, it cannot be determined whether the public prosecutor is indeed authorising the re-personalisation of passenger data.

#### On the accountability of the controller

- The controller does not sufficiently account for a number of data protection safeguards contained in the PNR Act and in the correspondingly applicable provisions of the Act on police data.
- It does not seem possible to ensure the accuracy and completeness of the unverified passenger data. The controller should investigate to what extent data quality can compromise the effectiveness of the PNR Act.

- The controller must still comply with the annual mandatory internal privacy audit and also carry-out information security audits relating to the Pi-NL.

#### With regard to internal and external supervision

- Other than in the PNR Directive, the independence of the Data Protection Officer is not protected by the PNR Act.
- The TRIP application still lacks some record-keeping functionalities, which impedes the Data Protection Officer's ability to supervise.

#### Regarding the rights of data subjects

- The question arises whether the current provision of information on the PNR Act on the webpage of the central government informs passengers about the PNR Act in clear and simple language.
- The controller must ensure that data subjects can exercise their right to access passenger data by secure means of communication.

**Research question 4:** *Based on the application of the PNR law in practice to date, what can be said about the effectiveness, necessity and proportionality of including in the scope of the law the mandatory transfer of passenger data on intra-EU flights?*

Since the entry into force of the PNR Act until 1 January 2021, 38.2 million passenger data have been collected from intra-EU flights. In 2020, the passenger data of 4,188 passengers who flew intra-EU were shared with the Dutch competent authorities. This is approximately 0.027% of all intra-EU passengers from whom data was collected. Of these, 2,224 were intra-EU passenger data that were disclosed at the request of the competent authorities. Proportionally, there are no more positive matches between passenger data from intra-EU flights and the SIS II database than there are for extra-EU passenger data.

##### *a. The effectiveness of the application of the PNR law to intra-EU flights*

For the purpose of this study, effectiveness is understood as the contribution to the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The quantitative data show that the intra-EU passenger data are suitable in practice for contributing to the prevention, detection, investigation and prosecution of terrorist offences and serious crime. However, the degree of effectiveness cannot be specified, also due to the short period of time the PNR law has been in force.

##### *b. The necessity and proportionality of applying the PNR law to intra-EU flights*

Considering proportionality and necessity, the quantitative data are interpreted in two contradictory ways. On the one hand, *bona fide* travellers are hardly affected since only 0.027% of intra-EU passengers' data have been provided to competent authorities by 2020. On the other hand, the personal data of a large group of persons not targeted by the PNR legislation are systematically collected and processed within its purpose. According to the competent authorities, the Ministry of Justice and Security and Europol, intra-EU passenger data are of great importance for criminal investigation purposes. However, the civil society organisations interviewed emphasise the disproportionate nature of the indiscriminate mass surveillance introduced by the PNR law.

It remains to some extent a normative assessment whether the indiscriminate collection, storage and use of passenger data of all passengers travelling by air, whether or not they cross the external borders of the EU, can be considered necessary and proportionate.

c. *The constitutional test of effectiveness, necessity and proportionality*

As implementing legislation for the PNR Directive, the Dutch PNR Act must comply with the principles of effectiveness, necessity and proportionality provided for in the EU Charter. The fate of the PNR Act, including its application to intra-EU flights, is inextricably linked to the legality of the PNR Directive.

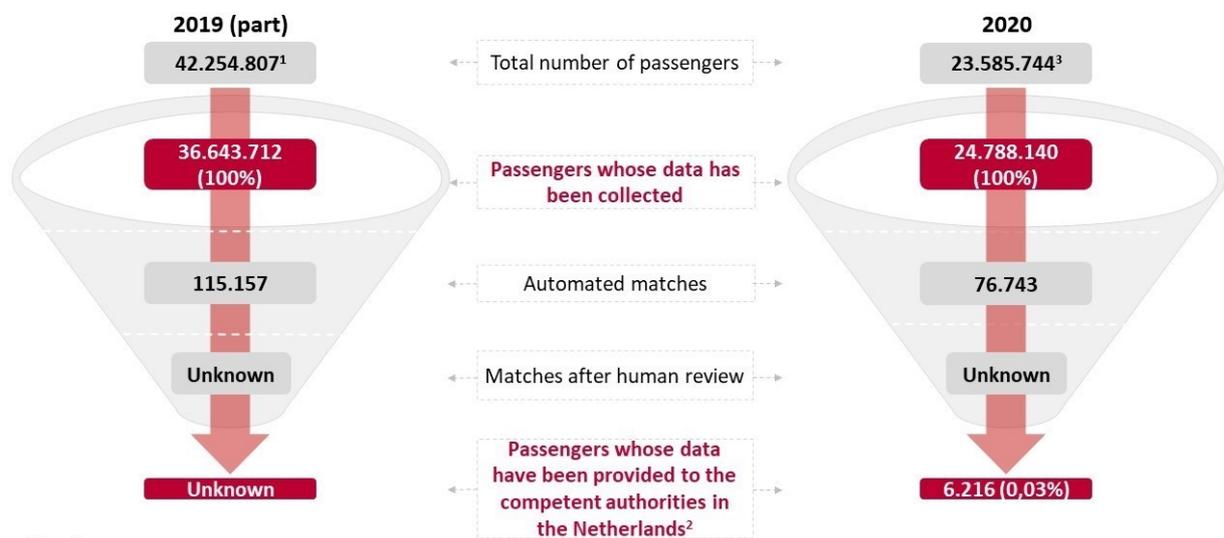
The Court of Justice of the European Union has been requested by a number of national courts to give a preliminary ruling on the compatibility of all or parts of the PNR Directive with Articles 7, 8 and 52(1) of the EU Charter. Besides a number of detailed issues, the fundamental question of the proportionality and necessity of the general and indiscriminate collection, retention and use of passenger data arises. A ruling of the Court on the pending request for a preliminary ruling from the Belgian Constitutional Court is expected before the sunset clause in Article 25a of the PNR law enters into force on 18 June 2022.

## Findings main question

The main question of the study concerns three aspects of the PNR law in practice: its **use**, its **effectiveness** and its **impact**.

The use of the PNR Act can be shown in quantitative terms. The quantitative data shows that from the entry into force on 18 June 2019 to 1 January 2021, airlines have shared the data of 61.4 million passengers with the Pi-NL. Of about 0.025% of the passengers whose data has been shared with the Pi-NL, passenger data is also provided to competent authorities in the Netherlands.

Figure 2 (below) contains a graphical overview of the use of passenger data in figures.



<sup>1</sup> From July 2019

<sup>2</sup> Number of passengers whose data has been transmitted to other EU Member States, third countries or Europol is unknown.

<sup>3</sup> Due to the impact of COVID-19, the total in 2020 is lower than in 2019. Due to the high number of cancellations, a lot of passenger data has also been received from cancelled flights so the number of passengers for whom data was collected is above the total number of passengers.

Figure 2. *The processing of passenger data in figures.*

While the input of passenger data provided for the purpose of the review is known, information on the resulting output is lacking. To some extent, the demand for passenger data by competent authorities is an indicator of its **use**, but it says nothing about its results and impact in the fight against terrorist offences and serious crime.

With regard to the **effectiveness** of the PNR Act, the interviews conducted for this study lead to the conclusion that the sharing of passenger data with competent authorities has, in several cases, contributed to the purpose of the Act. No conclusions can be drawn as to the level of effectiveness and to what extent the same results could have been achieved without the PNR Act.

Based on the interviews conducted for this study, the perceived usefulness of passenger data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes can be illustrated. The competent authorities consider requesting of passenger data from the Pi-NL for offences under Annex 2 of the PNR Act as one of the tools in the toolbox for digital investigation. Passenger data accessible under the PNR Act not only provide insight into travel movements across various airlines, but is also used to discover who paid for and booked a flight and who travelled with whom. Passenger data is also useful to retrieve current information of criminal suspects and to make tactical choices in a criminal investigation.

The PNR Act has an **impact** both on the work of the law enforcement agencies and on the fundamental rights of the passengers concerned. The creation of the Pi-NL as a single information point for the collection, processing and transfer of the passenger data within the purpose of the PNR Act facilitates the demand for such data by the competent authorities. The PNR Act also allows new investigatory possibilities, for example to assess, prior to the planned arrival in or departure from the Netherlands, whether passengers should be subject to further examination due to possible involvement in a terrorist offence or serious crime. At EU level, the PNR legal framework has facilitated cooperation and exchange of passenger data.

The blanket and indiscriminate collection, use and long-term storage of passenger data must not only be effective, but must also comply with the principles of necessity and proportionality. For air passengers, the PNR Act means the collection and storage of personal data of a large group of persons who are not targeted by law enforcement, which appears to be disproportionate from this point of view.

Finally, the fate of the PNR Act is closely linked to the fate of the PNR Directive, which is currently in the hands of the Court of Justice of the European Union. A ruling from the Court in the pending request for a preliminary ruling from the Belgian Constitutional Court is expected before the sunset clause in Article 25a PNR law enters into force on 18 June 2022.