Panteia
Research to Progress

Research voor Beleid | EIM | NEA | IOO | Stratus | IPM

Gebruik van passagiersgegevens voor grenscontrole

Evaluatie van de uitvoering van de API-richtlijn

Auteurs:
Guido Brummelkamp
René Vogels

Zoetermeer, 11 december 2018

Summary

Study background

In order to improve border controls and prevent illegal immigration airline companies are obliged to provide the authorities responsible for border control with certain personal details from passengers and cabin crew arriving from outside the Schengen and European Union area. In the Netherlands, the body responsible for guarding national borders is the Royal Netherlands Marechausee, henceforth referred to as KMar. The KMar receives personal details from an individual's travel document, and these details are supplemented by certain details concerning the flight and the booking process. These details are known as Advance Passenger Information (API). In this context, 'advance' refers to the moment at which these details must be provided, namely, at the end of the boarding process. By adopting this approach to the provision of personal details, the Netherlands implements and adheres to the requirement in the European Directive on the obligation of carriers to communicate passenger data (Directive 2004/82/EG). The requirement concerning personal information has been transposed into the Dutch Vreemdelingenwet 2000 (Alien act).

This current study evaluates the use of API-data in the Netherlands. The research is a follow-up study to the evaluation of API conducted in 2014. At that time, the API-system was still being developed. Based on the first evaluation study of the system, the Minister promised the Dutch national parliament that a second evaluation study would be conducted once the system was fully developed.

For this second evaluation study, two main research questions have been formulated:

- What can be said regarding the use and the effectiveness of API-details in aid of border controls and the prevention of illegal immigrants, and in which way have earlier recommendations regarding the API been considered?
- To what extent can recent relevant European developments have an impact on the way in which the Netherlands uses API data?

As part of this study, a literature review phase has been conducted, along with a series of interviews with:

- representatives from three Dutch airlines and the international sector organisation for air transport (the IATA),
- employees from KMar.
- policy makers from relevant ministries,
- and a scientific researcher.

The study also entailed a quantitative component, which involved examining counts per month for the period of November 2013 to March of 2018. These counts were not available for the entire period, nor are they comparable for that period. The reason for this being that there have been changes in the number of airports where the API requirement was in place. To gain an accurate impression of the way in which API works in practice, members of the research team joined KMar employees

on the work floor. Based on the two mornings during which the researchers joined the KMar, several cases have been developed and included in the report for this study.

Use of API details

In order to answer the first research question, the study first describes how exactly API details are expected to contribute to more effective border controls and the prevention of illegal immigration. The KMar obtains the passenger data following the controls and inspections that take place in the boarding process when taking a flight to the Netherlands. Airline companies collect and check the data and send these to the KMar when the flight has departed. API data are based on passport information and contain supplementary details about the flight and the booking itself.

Based on the API data, the KMar can evaluate the individuals on board the flight by checking whether any of the individuals appear in any of the various international and national detection databases, or on watchlists or match with a profile based on their personal and flight details. A risk profile can be based on different variables. For example, the combination of the size of the travelling party, the country of departure, nationality, age, and gender can all play a role.

The screening involved in this evaluation process is carried out by the API Centre, a component of the Target Centre Borders. The department A&O (Analysis & Research) contributes to the screening process by, for instance, providing the API centre with profiles. The screening process leads to so-called 'matches'. In those situations, the API data match with a detection database or profiles. These matches are then examined in further detail and validated, and are then referred to as a 'hit' if the passenger requires additional attention at the gate or at the border. Any given hit involves, among other things, the checking of personal details, and establishing whether the detection is still relevant. During this phase, additional details can be linked to the hit. The additional details may take various forms, such as a photograph, or an anticipated approach to treating the case. In situations where the API Centre establishes that a hit has indeed been identified, it then sends instructions to the operational organisation that an intervention must take place. These instructions are referred to as alerts, and can involve different types of action. In order to respond to alerts, the KMar houses a mobile team for Dedicated Gate Control (DGC) alongside its regular border control branch. The DGC can then await and intercept passengers for whom an alert has been made at the airport gate. Thus, the KMar can take action in a timely fashion due to the API data and the analysis of those data.

The number of alerts has steadily increased in recent years from some 200 alerts a month in 2013, to more than 1,100 alerts a month during the first three months of 2018. This trend follows the general increase in border traffic relating to flights were API requirements apply, and the fact that from the 1st of June 2016 onwards, all airports outside of the Schengen zone needed to provide API data. Before that time, the requirement of delivering API data was limited to 54 airports. The

number of alerts is equal to around 0.1% of the total number of passengers that enter the Netherlands form outside the Schengen area. The percentage differs slightly from month to month. During the first three months of 2018, this proportion increased slightly to just over 0.1%. The total number of passengers differs per month as well; in 2017 and during the first quarter of 2018, there were on average some 1 million passengers per month.

Effectiveness of API

The number of alerts which relate to (the risk of) illegal immigration was around 421 passengers in 2017 (which is equivalent to 3.6% of all alerts in that year). In 2017, there were around 120 instances where an alert and the connected database analyses have led to a person being denied entry to the Netherlands (Schengen). Around 14% of the alerts applies to passengers whose travel document has been lost of is registered as stolen.

A large part of all alerts (38%) concern passengers who have been detected because they have so-called 'Mulderfeiten' (traffic fines in The Netherlands) on their personal dossier that have not (yet) been resolved. For example, if a passenger has one or more unpaid traffic tickets, despite several requests for payment, they may be detected.

The KMar employees who are involved with border controls on a daily basis emphasise the worth and utility of API. They indicate that the API details contribute to more effective border control.

The added value of the API details are threefold:

- First of all, there is more time to compare passenger data based on databases and risk indicators as the data are available from the moment that the airplane departs. Furthermore, there is more time and opportunity to consult colleagues regarding a hit. KMar follows a four-eye principle; there is always a second individual who assess a hit. In cases concerning an alert with high urgency, the DGC's mobile team can be informed in order to intercept the passenger in question at the gate.
- Secondly, the API centre can report irregularities and risks that are not examined at a border post. The API centre has broader insight in this respect. The API centre can, for instance, see if a passenger travels using an irregular route, or whether a passenger is accompanied by surprising or unusual travellers. These sorts of irregularities can be an indication of a heightened risk of illegal immigration, and can constitute a reason for asking the passenger pointed questions when they arrive in the Netherlands.
- Thirdly, the API data provide added value as the control procedures at the borders are improved and made quicker as passenger details are available for examination beforehand. The controls and the entry points can be used only for the identification of passengers and the validity of their travel document. This improves the flow of travellers and prevents long lines and waiting at the entry points, and this is an important added value for airlines and passengers. Without API, the KMar would have to compare the details of all passengers to detection databases and lists at and after the arrival of passengers in the Netherlands.

The researchers identify three important considerations in the use of API details.

- Alerts are transferred manually to the enter points. The alerts are printed out by the group commanders for the entry points, and these group commanders ensure that the printouts of the alerts arrive at the desks of the border guards at the entry points. This way of working is relatively demanding in that it relies strongly on the attentiveness and alertness of the border guards. These individuals are expected to receive the printed information regarding the alerts, to understand and retain the information, and to actually recognise the passengers concerned when they try to cross the border. According to KMar employees involved with this process, the border guards are sufficiently alert and attentive. However, it goes beyond the scope of this research to establish to what extent that is indeed the case, or to establish how often passengers for whom alerts have been disseminated, are not intercepted in practice.
- API details offer more possibilities to detect passengers beyond purely comparing their details with detection databases. Passengers who have not been detected or signalled in a database or detection system may still warrant further attention. This issue applies mainly to the detection of 'unknown persons with an unknown risk', who can be filtered out of the flow of passengers based on their personal and travel details. This process is currently conducted manually. However, steps are currently being made to automate this process by, for example, using algorithms which systematically search for irregular patterns, or deviations from standard patterns.
- The third consideration relates to the understanding amongst airline companies as well as third parties who use these API data and must therefore adhere to the various requirements concerning the strict division between the currently API requirements, and the PNR Law currently under development. The PNR Law states that the airline companies must deliver Passenger Name Record (PNR) data. The PNR data include information that the airline companies need to make, process and check a reservation. Besides personal details such as the name and date of birth, the PNR data also include payment details, travel companions, baggage, and seating place in the airplane. The PNR Law was formally proposed in the national parliament on the 9th of January 2018. In the event that this law passes, airline companies will be obliged to collect data for each passenger and to pass these data on to two separate booths; once to the API Centre in the same manner as now, and three times to the Pi-NL booth. The Pi-NL booth requires PNR data as well as API data.

The fact that airline companies would need to provide API as well as PNR data (now only to the Customs and in future also based on the PNR-legislation) to the government does raise certain questions amongst airline companies regarding the efficiency and effectiveness of the new requirement. In other places in the world, the general practice is that there is one booth for passenger information; this is the case in the United States and the Gulf States, for instance. Airline companies in the Netherlands, as well as the sectoral organisation the IATA, lobby for a single window instead. If the PNR Law is passed and accepted, the Dutch authorities must collect passenger data using two channels, which forms an extra administrative burden for airline companies. The Dutch government is exploring the option of a single window to transfer the passenger information data.

Results of European developments

The API directive is part of a broader package of European measures to strengthen the borders of the internal market. API was the first element of this package. These measures arise in large part due to the pointed increase in the number of passengers entering Europe from third countries, and this trend is expected to be continued in the coming years (from 50 million non-EU passengers in 2015 to 76 million in 2025). The combination of having more passengers, as well as higher safety requirements have triggered the search for possibilities as to checking and processing large flows of passengers, without having to make concessions regarding safety requirements, or in respecting the rights of the passengers.

A few important recent developments and measures are brought together under the policy direction 'Smart Borders'. The measures involved include amongst others:

- Entry-Exit System (EES): In November of 2017, the Council of the European Union decided to introduce an EES, which would register all attempts by non-EU citizens, and non-registered EU citizens travelling into the Schengen area.
- European Travel Information and Authorization System (ETIAS): The Council of the European accepted a regulation on September 5th, 2018, stating that a European system for travel information and authorisation would be set up. The system is to be similar to the American Electronic System for Travel Authorization (ESTA). The system means that subjects of a third country who do not need a visa, must request travel authorization before they can travel into the Schengen zone.
- Systematic border control based on databases: On the 7th of March 2017, the Council for the European Union has accepted an amendment to the Schengen border code to sharpen the controls at the outer borders of the zone. The Member States will be obliged to systematically check all individuals at the borders of Schengen using relevant databases.
- Interoperability: Within the EU, work is being done to improve the interoperability of information systems such as EES, Visa Information System (VIS), ETIAS, and Schengen Information System (SISII). The rationale is that these systems will align with one another and allow for databases and systems to better use each other's information.
- Improving SISII: New categories for signalling and detecting are being added to the SISII.

When implementing EES and ETIAS it will be important in the context of carrier liability for airline companies to be able to assess whether someone has an ETIAS travel authorisation, and to be able to see whether the term of 90 days has not passed. Carrier liability entails being able to make the airline company accountable and responsible for ensuring that an individual is provided with a return flight in the event that they are not allowed into the Netherlands.

Comparable systems that check whether a passenger is permitted to cross the border of their country of destination before the departure of their flight are already in use in the United States, Canada, and Australia. These countries fall beyond the scope of the European API Directive, but can provide a possible approach that the EU could apply regarding the combined use of details and registers to assess the entrance of passengers. Airline companies receive an OK/NOT OK TO

BOARD signal before they board a plane. In doing so it is immediately clear whether a person will or will not be allowed to travel to the country of destination, and this reduces the risk to airline companies that they be made responsible for providing return flights for those passengers. Furthermore, this could contribute to the increase of safety on board because potentially dangerous individuals are not allowed on planes to begin with due to the existence of detection files and lists of risky individuals.

The expectation, and certainly the desire of the airlines, is that in the longer term, a single window for the delivery of passenger data will become a globally applied model. This is already the case in several countries. The API obligations are now included in the Netherlands in the Vreemdelingenwet 2000 and also apply to Dutch passengers. PNR-data are currently provided to the Customs and in the future also based on the PNR-legislation for the prevention and detection of serious crime and terrorism. Embedding the API and PNR obligations in one framework law on Civil Aviation Safety is, in our view, a logical route for the future. This would certainly increase the transparency for all parties involved.