ON API

What legislative and operational measures have you undertaken to establish an Advance Passenger Information (API) system?

Answer

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) since 2007. The requirement concerning personal information has been transposed into the Dutch Vreemdelingenwet 2000 (Alien Law). For flights that arrive from outside the Schengen and European Union area, airline companies are obliged to provide the authorities responsible for border control with certain personal details from passengers and cabin crew.

In the Netherlands, the organisation responsible for guarding the Schengen borders is the Royal Netherlands Marechaussee, henceforth referred to as KMar. Airline companies collect and check the data and send these to the KMar when the flight has departed. 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 In formation (API). Based on the API data, the KMar can evaluate the individuals on board of 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.

This evaluation of individuals based on API data is carried out by the API Center, a component of the Targeting Center Borders. In situations where the API Center establishes that a hit has indeed been identified, it then sends instructions to the operational organization 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.

If such a system has already been put into place, how many cases were detected and promptly notified so far to relevant authorities of other countries and international organizations?

Answer:

An API system is in place (see above).

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 or is registered as stolen.

If such a system has not yet been put into place, why is that the case and how does the Government intend to swiftly make them operational?

Answer:

Not relevant since system is in place. See above.

How is the Government ensuring that the collection, analysis and sharing of API does not violate relevant human rights and fundamental freedoms?

Answer

The collection of API is according to the API-guideline. This is implemented in the Dutch Aliens Law 2000, to which the GDPR is applicable.

ON PNR

What legislative and operational measures have you undertaken to develop your capability to collect, process and analyze Passenger Name Record (PNR) data, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offences and related travel, and to share such data with relevant States?

Answer

The implementation of the PNR-guideline (EU Directive 2016/681) is currently being considered by parliament. The Dutch Passenger Information Unit (Pi-NL) will be operational once the legislation has been adopted. The Pi-NL has the operational capacity to collect, process and analyse PNR data. As described in the PNR directive and the national legislation for implementation of the PNR directive the Pi-NL will ensure full respect for fundamental rights and fundamental freedoms.

What challenges are you facing in setting such capacity?

Answer

Once the PNR-legislation has been adopted the Pi-NL has the full capacity to collect, process and analyse PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

How is the Government ensuring that the collection, analysis and sharing of PNR does not violate relevant human rights and fundamental freedoms*?*

Answer

All measures, as described by the EU PNR Directive (2016/681), will be put in place to prevent the violation of relevant human rights and fundamental freedoms. The Directive specifically describes that PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. A data protection officer will be responsible for monitoring the processing of PNR data and implementing relevant safeguards. PNR data will be depersonalised after six months and deleted after five years. The Directive prohibits the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the Pi-NL, they shall be deleted immediately.

ON BIOMETRICS

What legislative and operational measures have you undertaken to develop and implement systems to collect biometric data to responsibly identify terrorists?

Answer

The National Police and KMar are authorized and equipped to use biometric data to identify suspected terrorists.
The Netherlands participates in several European agreements such as Eurodac, EU-VIS (Alien law) and Prüm (Criminal law). In Eurodac and EU-VIS the fingerprints of third country nationals are compared to the databases. EU-vis is checked at all border crossings for third country nationals who have visa requirements.
With Prüm it is possible to make a search with fingerprints and/or DNA in the criminal database of the participating countries. One of the goals of Prüm is taking countermeasures against terrorism, illegal migration and other border crossing crimes.
In 2018 an amendment to the Penal Code, the Code of Criminal Procedure and some other laws to strengthen the criminal and criminal prosecution possibilities to combat terrorism passed (strengthening the criminal law approach to terrorism). The law extends the possibilities of taking cell material for DNA testing from suspects of terrorist crimes.

What challenges are you facing in setting such capacity?

Answer

does not apply

Are you sharing this data with other States, with INTERPOL and with other relevant international bodies?

Besides the legal opportunities offered by Prum, it is possible to share this data with other states for law enforcement purposes on the basis of legal aid.

How do you ensure that the collection and exchange of biometrics is carried out in compliance with domestic and international human rights law?

Answer

In such cases the National Police and KMar act according to the applicable legal frameworks. To ensure compliance with domestic and international human right law the responsible organizations perform Privacy Impact Assessments (PIA) and the respective organizations only use systems that are compliance with the applicable legal framework.
The collecting of cell material for DNA research is an infringement of the right to private life, protected by Article 8 ECHR. The measure may be justified according to the case-law of the European Court of Human Rights, particularly in the context of the investigation into crimes of a certain gravity (see ECHR 4 December 2008, app. 30562/04 and 30566/04; S. and Marper v. United Kingdom). The ECHR makes no further demands on the degree of suspicion. In general, however, restrictive rules must be imposed on the retention of the obtained data in a DNA database. The Dutch legislation meets that requirement.