Organization for Security and Co-operation in Europe

SEC.GAL/190/18
3 December 2018

ENGLISH only

Outcome Document from the 2nd OSCE-wide Seminar on Passenger Data Exchange

Vienna, 1-2 November 2018

Venue:
Ratsaal in Hofburg, 5th floor
Hofburg Congress Centre, Heldenplatz, 1010 Vienna

Organization for Security and Co-operation in Europe

1. United Nations Security Council Resolution 2396: A global framework for action

Foreign terrorist fighters (FTFs) pose a serious threat to States, given the risk that they may carry out attacks at home or engage in recruitment efforts. That is why, in December 2017, the United Nations Security Council unanimously adopted Resolution 2396. Building upon previous Resolutions 2178 (2014) and 2309 (2016), 2396 aims at helping States in detecting and countering the movement of FTFs, especially those returning or relocating from conflict zones.

2396 creates **three main obligations for States in the area of border security**.

1. To collect Advance Passenger Information (API) and Passenger Name Record (PNR).

2. To develop systems to collect biometric data.

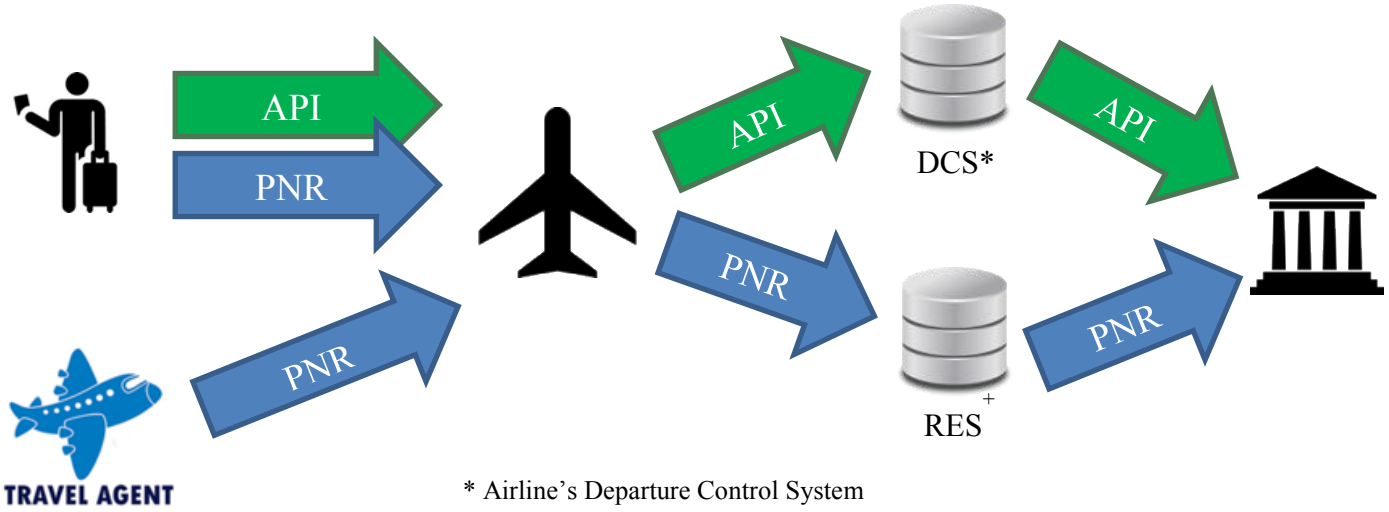
3. To share this information bilaterally and multilaterally including by using databases such as those of INTERPOL.

Resolution 2396 was adopted under Chapter VII of the United Nations (UN) Charter, which makes compliance with these obligations mandatory for all Member States. However, not all States have the resources or the capacity necessary to do so. That is why Resolution 2396 calls upon States, UN bodies and international and regional organizations to provide technical assistance, capacity-building and support to those countries that request it.

Full implementation of Resolution 2396 represents a massive undertaking. To date, **only 48%** of OSCE participating States have set up an API system, while **just 29%** collect PNR data.

2. Overview of passenger data: what are API, PNR and iAPI?

API and PNR are both types of passenger data collected by airlines. When an API or a PNR system are in place, details of passengers are transmitted by airlines to law enforcement authorities before a flight's departure or arrival at the airport of destination.



* Airline's Departure Control System

\+ Airline's Reservation System

API and PNR data are not quite the same

API is the biographic information contained in the Machine Readable Zone of a passenger's travel document submitted during check-in.

API is based on a government-issued travel document and thus it is verified data.

API is useful for matching against watch-lists and risk profiles and detecting whether inadmissible persons are attempting to travel.

PNR is the data provided when booking a flight, including contact details and payment information.

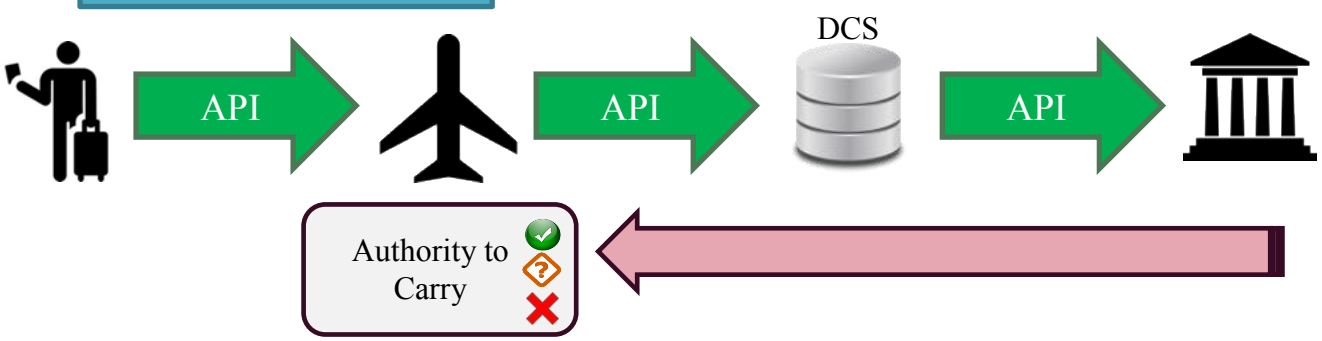
PNR is manually input by the traveller or the travel agent and not verified.

PNR can help to identify suspicious travel patterns and hidden connections between known threats and their unknown associates by examining specific data elements, such as credit card numbers.

In addition, API systems can be divided in two distinct categories: non-interactive batch-style API systems and interactive API (iAPI) systems. In a batch-style API system, information from passengers are collected during the check-in process and then communicated together in a single message.

An iAPI system allows for a two-way communication in near real-time. The airlines transmit the API message on a per-person basis to the requesting authorities at the time of check-in, while law enforcement agencies have the opportunity to decide whether a certain person is allowed or not to board a plane by issuing a board/no-board message.

Interactive API (iAPI)



Pros of iAPI

1. Governments can prevent the arrival of inadmissible persons

2. Airlines do not have to cover costs of detention and return

Cons of iAPI

1. iAPI systems are far more complex than batch style systems

2. Higher development, implementation and operational costs

To learn more about the different types of passenger data exchange systems, please watch the online videos included in the International Air Transport Association's (IATA) Passenger Data Toolkit.

Organization for Security and Co-operation in Europe

3. How to set up an API/PNR system?

There are six key steps that need to be followed to set up an API/PNR system. These are based on the IATA Passenger Data Toolkit and should be seen as a checklist:

1. Create an Interagency Working Group

- It should be formed by representatives of all the agencies and Ministries that are going to be involved in passenger processing.
- Among other issues, it will be responsible for deciding on the specific system to be implemented (either batch-style API, iAPI, or PNR) and determining the costs and budget for the establishment of the system.

2. Develop appropriate legislation

- A legal framework for data capture, transfer and storage is needed for law enforcement authorities to be able to obtain passenger data from airlines. Because API and PNR serve different purposes, different laws should be drafted for each type of data.
- All legal provisions should comply with existing international standards, namely ICAO's Annex 9 to the Chicago Convention, the WCO/IATA/ICAO Guidelines on API, and the ICAO Guidelines on PNR.
- For more information, please read Sections 5 and 6 of last year's Outcome Document.

3. Set up a 'single window' or a Passenger Information Unit

- If you develop an API system, you should ensure that there will only be one government authority receiving passenger data on behalf of all other authorities, functioning as a 'single window'. This may require legislative reform to allow for inter-agency information exchange.

The Passenger Information Unit (PIU)'s central role

The European Union's PNR Directive mandates all EU Member States to establish special entities – the PIUs – responsible to collect, store and process PNR data received from carriers. At the PIU, passenger information is also cross-checked against databases and alerts are validated and issued based on pre-determined risk analysis criteria. These alerts are then sent to the competent authority for taking appropriate action.

The PIU should have a **programme branch** and an **operations branch**. The former is responsible for providing policy direction and ensuring programme consistency, while the latter implements the priorities set by the programme branch, provides support to stakeholders (e.g. airlines) and ensures that the staff are familiar with passenger data and the PIU working processes.

For more information on how to set up a PIU, please look at pp. 13-15 of this WCO guidance document.

4. Engage with airlines

- Communication with airline stakeholders should start as soon as a decision is made to implement an API or PNR system. By doing so, you will be able to know what can and cannot be acomplished with airlines' existing systems.
- For more information in this regard, please refer to Section 7 of last year's Outcome Document.

5. Invite IT service providers to meetings

- A key question that States need to address is how to obtain the data from the airlines. If an external solution is needed, authorities should send invitations to relevant service providers to meet with the project team and present their solutions and competence in this field.
- The purpose of these meetings is not to select a solution, but to verify each provider's capabilities and experience.

6. Manage a tendering process

- A Request for Proposals (RFP) should be then issued to identify the desired supplier. This process includes defining scoring criteria to fairly assess each provider based on the government's needs as well as evaluating the providers' proposals.
- The OSCE can provide support with issuing an RFP, managing the tendering process and making recommendations about the final result through an independent consultant.

4. Best practices and challenges in the implementation and exploitation of API and PNR systems

It is advisable to follow a **phased implementation approach**. Setting up an API or a PNR system is not easy. Several tests will have to be conducted to make sure that airlines are sending you the data you need and at the right time. Therefore, it is better to start working with one airline or even one route and, once all connectivity challenges have been overcome, gradually connect the rest of the airlines to your system.

It is essential to **make sure that your implementation strategy is aligned with international standards**. In terms of timing, it is easier for airlines to comply with passenger data exchange systems that follow global standards, which will result in lower costs and faster implementation (3-6 months instead of 24-36 months).

The best API and PNR programmes are those that **involve all national agencies that will make use of passenger data** (Border Police, Customs, Intelligence Services, etc.) **early in the project**. Make sure to work closely with **data protection experts** who can advise you on how to draft an API/PNR law or amend your existing legislation in order to protect the travellers' right to privacy.

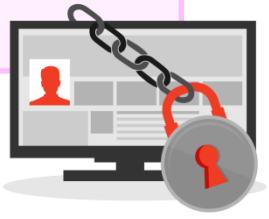
States should always **test the risk profiles** they will use for cross-checking passenger data to make sure that they are adequate to their needs. It is also recommended to **conduct audits on the effectiveness of your passenger data exchange systems**. Certain participating States have produced guidelines for developing risk scenarios, while others publish online the results of the internal audits of their border management solutions.

There are **two main ways of setting up an API/PNR solution**. One is to develop it yourself – the other one, to rely on an external partner. There are advantages and downsides to both of these alternatives. On the one hand, developing your own solution can be cheaper, but you need well-trained staff with the capacity and skills required to build these systems. On the other hand, it might be faster and easier to engage with an external IT provider with previous experience on setting up these programmes.

Certain **OSCE participating States stand ready to provide support for API and PNR implementation to other countries**. Australia, Bulgaria, France, or Lithuania are willing to host study visits, share legislation and technical implementation guides, deliver lectures and trainings, and provide mentoring. A list of States who offered support during the OSCE-wide Seminar is provided in Section 9 below.

You can also **engage with international organizations or States that offer IT tools for free**. Luxembourg has developed the API-PNR Gateway, a platform that works as a single point for the collection of passenger data that is available for all EU Member States to join. The UN Office on Counter-Terrorism has started implementing a five-year capacity building project on API and PNR that includes the donation of an IT-software solution for processing data and free support and maintenance. The United States is offering its Automated Targeting System-Global (ATS-G) to States. This is another supported IT-software solution that is available for free through an information-sharing agreement. The World Customs Organization also offer software to customs authorities for analyzing API and PNR data. Contact details can be found in Section 9 below.

Unfortunately, **there is no internationally harmonized legal framework to overcome conflicts of law pertaining to data privacy and the transfer of PNR data**. As a result, disagreements between States on how to appropriately handle sensitive data and what safeguards should be put in place for protecting passengers' right to privacy and ensuring data protection and non-discrimination must be dealt with bilaterally. In order to be able to collect, store, process, and exchange PNR information both internally and externally, international agreements and/or Memoranda of Understanding will have to be signed with other States.

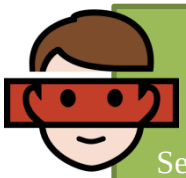


5. Biometrics: what are they and why are they useful?

Biometric identifiers are distinctive and measurable characteristics that are used to label and describe individuals. They are often related to physical attributes of the body, like fingerprints, DNA, or face recognition. However, they also include behavioural characteristics, such as the way we talk or the way we type on our computers.

The importance of biometric data lies in the fact that many of these characteristics are unique. In other words – facial measurements, the patterns that your veins make and even the way you walk – all of these attributes vary from one individual to the other.

This uniqueness is the reason why biometrics are increasingly used for border management and counter-terrorism purposes, as they can help law enforcement authorities determine someone's identity with absolute certainty.



e-Gates: An example of a biometric border tool

Several airports across the OSCE area have set up e-Gates. These gates scan electronic passports and compare the biometric information in the chip of the passport against a live scan of the traveller's face using facial recognition technology. If the traveller is using someone else's passport, the border guards will know.

States are also using biometrics techniques within forensic science. Forensic biometrics is useful not only because it provides an identification, but also because it can prove or disprove someone's involvement in a crime. It can link a person to an activity, an event, a location or another person before, during or after an incident.

However, even if biometric data can be an essential tool for combatting terrorism, it is equally important to make sure that the collection, the use and the exchange of this information is done in a responsible way.

6. Data privacy implications and other challenges related to biometrics

States must address the human rights implications of biometrics and make sure that biometric capturing and processing is carried out in accordance with international law obligations

Data Processing	States must nominate a data controller who will be responsible for managing all data processing activities. He/She will retain responsibility even if the data processing function is outsourced.
Data Sharing	The sharing of data must be approved domestically and subject to a clear legal framework. Biometrics can be shared only with trusted recipients and for the purposes included in the law.
Preventing Data Misuse	States must secure all biometrics information from unauthorized access and misuse, as well as to ensure that the data is accurate and that it has been provided without malevolent intentions.
Oversight	Effective and impartial oversight mechanisms by an independent body to which individuals can have access must be put in place to prevent the arbitrary collection and storage of biometrics.

For more information, please read the UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism.

Despite the usefulness of biometrics and the international obligations outlined in Resolution 2396, it will take many years for all States to be able to securely collect and store biometric data due to limited capacity and resources.

Prior to the Seminar, the OSCE shared a questionnaire with participating States to determine their level of compliance with Resolution 2396 in relation to biometrics collection. These are the two main takeaways from the exercise:

There is a **lack of coherence among biometric systems** in the OSCE area as a result of an **absence of international standards** regarding the collection of biometric information.

Even within one country, there is no uniform approach to biometric data collection. In most cases, it only takes place at major airports. But even when biometrics are collected, some border crossing points do not perform biometric watchlists search nor biometric information

For example, there is no common approach regarding the minimum age for the collection of fingerprints – it varies from 12 to 18 years old depending on the country – or the storage of biometric information – in some States, biometric data is not stored; in other, it is kept until a person turns 100 years old.

7. The importance of intra- and inter-State information sharing

While the collection of passenger and biometric information is a key element for an effective counter-terrorism strategy, this information, on its own, is just data. The added-value of it is to establish automated cross-checking of this data against national, regional and international watch lists, as well as to share this information internally with all relevant domestic law enforcement agencies.

2396 calls upon States to **enhance intra- and inter-State co-operation** by:

1. Ensuring that domestic law enforcement, intelligence and counterterrorism agencies are connected to national, regional and international databases, such as those of INTERPOL, and exchange appropriate information related to FTFs.

2. Sharing with other States information related to watchlists or databases of known and suspected terrorists that include biometric data, in compliance with domestic and international human rights law.

During the Seminar, several options were discussed to promote compliance with Resolution 2396's obligations related to information exchange:

1. Request INTERPOL's support to integrate their latest web services

Technical solutions like MIND/FIND enable frontline law enforcement agencies to run checks against INTERPOL's Stolen and Lost Travel Documents (SLTD) and receive an instant response.

The implementation of Web Services for Data Management (WISDM) allows States to automatically populate INTERPOL's databases.

2. Consider national and regional good practices for setting-up information exchange systems tailored to your needs

The United States' Department for Homeland Security (DHS) has developed a system for vetting immigration applications. The Secure Real Time Platform, which the DHS has been working to deploy with other countries since 2013, allows foreign governments to submit biometric data on applicants for comparison against the agency's own biometric data for border screening.

8. The OSCE's work in promoting compliance with Resolution 2396

In relation to API and PNR, the OSCE Transnational Threats Department (TNTD) has been organizing Workshops on Establishing a Passenger Data Exchange System across the OSCE area. To date, TNTD has travelled to Belgrade, Podgorica, Tirana, Skopje, Prishtinë/Priština, Bishkek, Tbilisi, Tashkent, Ashgabat and Chisinau to work with local authorities to prepare tailored Action Plans outlining the main steps they need to follow to implement API and PNR systems. These workshops are being followed-up with consultations aimed at supporting local authorities in implementing the Action Plans. This includes the provision of legal advice and technical and operational assistance by an independent consultant.

TNTD will continue organizing workshops and consultations throughout 2019. If you believe that such an activity is of interest to your participating State, please get in touch with Mr. Simon Deignan (simon.deignan@osce.org) to consider the possibility of organizing an event in your capital.

With regards to biometrics, TNTD has been supporting States to develop biometric passports and joining the ICAO Public Key Directory, a repository that allows countries to verify the biometric and biographic data in the chip of the passport. In 2019, TNTD will organize a series of country visits across South Eastern Europe to encourage decision-makers to join the PKD, which will be followed by the provision of practical guidance and operational support for developing national compatibilities with the PKD.

To address some of the challenges related to the collection and processing of biometrics for law enforcement purposes mentioned in Section 6, TNTD and the Biometrics Institute will jointly organize an OSCE-wide Seminar on best practices in the use of biometric data in countering terrorism from 11 to 12 April 2019.

The OSCE has also been very active in promoting information sharing. Nationally, TNTD supports the creation of police-customs co-operation centres and integrated border

management strategies. To facilitate the exchange of information and best practices between national border services, the OSCE has a Borders Network of National Focal Points (NFP) comprised of 103 contact points from 53 participating States.

TNTD's plans for 2019 include the setting up of new police-customs co-operation centres, contributing to the expansion and use of INTERPOL's databases, and the organization of thematic meetings for the NFP.

9. Who can I contact to get further information?

OSCE

Simon Deignan (simon.deignan@osce.org); Adrián Carbajo (Adrian.CarbajoAriza@osce.org)

IT service providers present at the Seminar

-Agile Borders (Andrew Priestley: andrew.priestley@agileborders.com)
-Amadeus (Peter Butler: pbutler@amadeus.com)
-DATI Group (Guntars Krēsliņš: Guntars.kreslins@kc.lv; Zvonimir Vuković: Zvonimir.vukovic@span.eu)
-IBM (Paul McKeown: paul_mckeown@uk.ibm.com)
-Idemia (Noureddine Ghamri: noureddine.ghamri@idemia.com)
-Rockwell Collins (Jon Floyd: jon.floyd@arinc.com)
-SITA (Andy Smith: andy.smith@sita.aero; Dmitry Taranka: dmitry.taranka@sita.aero)
-WCC Smart Search and Match (Justus Heuzeveldt: jheuzeveldt@wcc-group.com; Amr Rahwan: arahwan@wcc-group.com; Roelof Troost: rtroost@wcc-group.com)

OSCE participating States offering advice and support

-Bulgaria (Shteryu Bozhikov: Shteryu.Bozhikov@piu.bg)
-France (Christophe Hypolite: christophe.hypolite@interieur.gouv.fr)
-Georgia (Otari Khvedelidze: o.khvedelidze@rs.ge)
-Hungary (Szabolcs Deli: inter@tibek.gov.hu)
-Kyrgyzstan (Adylbek Kadyraliev: adylbek.kg@gmail.com)
-Luxembourg (Florent Goniva: florent.goniva@police.etat.lu)
-The Netherlands (Willem Mudde: WSC.Mudde@mindef.nl; Patrick van Doormaal: ptj.v.doormaal@mindef.nl)
-Slovakia (Lucia Szlobodova: Lucia.Szlobodova@minv.sk)
-United Kingdom (Ros Anchors: Ros.Anchors@homeoffice.gov.uk)
-United States (David Dodson: David.Dodson@cbp.dhs.gov; Michael Scardaville: Michael.Scardaville@hq.dhs.gov)

Airlines

-Austrian Airlines (Heinz Kermer: heinz.kermer@austrian.com)
-Lufthansa (Adel Baraghith: adel.baraghith@dlh.de; James-Patrick Sgueglia: james-patrick.sgueglia@dlh.de)
-United Airlines (Andres Hirschfeld: andres.hirschfeld@united.com; Beth Gehring: beth.gehring@united.com)

Other international organizations

-Biometrics Institute (Roger Baldwin: idtransnational@gmail.com)
-eu-LISA (Viktoria Skoularidou: viktoria.skoularidou@eulisa.europa.eu)
-IATA (Nuria Fermoso: fermoson@iata.org; Ilker Duzgoren: duzgoreni@iata.org)
-ICAO (Chris Hornek: chornek@icao.int)
-INTERPOL (Bozidar Popovic: b.popovic@interpol.int)
-IOM (Lívia Styp-Rekowska: lstyprekowska@iom.int; Dušica Živković: dzivkovic@iom.int)
-UNOCT (Ulrik Ahnfeldt-Mollerup: ahnfeldt.mollerup@un.org; Rocco Messina: messinar@un.org)
-WCO (Jin Randhawa: Jatinder.Randhawa@wcoomd.org)