Council of the
European Union

Brussels, 14 September 2020
(OR. en)

10720/20

IXIM 86
FRONT 238
JAI 691
AVIATION 158
COMIX 392

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 174 final
Subject:	COMMISSION STAFF WORKING DOCUMENT EVALUATION of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)

Delegations will find attached document SWD(2020) 174 final.

Encl.: SWD(2020) 174 final

EUROPEAN
COMMISSION

Brussels, 8.9.2020
SWD(2020) 174 final

COMMISSION STAFF WORKING DOCUMENT

EVALUATION

of the

Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)

{SWD(2020) 175 final}

Table of contents

Glossary

Term or acronym	*Meaning or definition*
Advance Passenger Information (API)	Information of an air passenger collected at check-in or at the time of online check-in. It includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight.
API - batch	An electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival and made available on the primary line at the airport of entry.[1]
Border control	The activity carried out at a border, in accordance with and for the purposes of Regulation (EU) 2016/399 (Schengen Borders Code)[2], in response exclusively to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance.
Border Crossing point	Any crossing point authorised by the competent authorities for the crossing of external borders.
Carrier	A natural or legal person who provides passenger transport services by air.[3]
Carrier gateway	Web service enabled system, to be introduced in accordance with Regulation 2018/1240 establishing European Travel Information and Authorisation System (ETIAS)[4], allowing carriers to verify the authorisation status of third-country national (TCN) travellers.
Charter flight/ Non-scheduled revenue flights (excluding on-demand flights)	Charter flights and special flights performed for remuneration other than those reported under scheduled flights. They *include* any items related to blocked-off charters and *exclude* air taxi, commercial business aviation or other on-demand revenue flights.[5]
Centralised Routing Mechanism	Central point to which air carriers may submit passengers and crew manifests and which can forward the passengers data to other information systems.

1 Annex 9 to the Convention on International Civil Aviation, Chapter 1.

2 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0399

3 Art. 2, Council Directive 2004/82/EC (API Directive) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082&from=EN

4 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1240

5 ICAO Glossary, https://www.icao.int/dataplus_archive/documents/glossary.docx

Competent authorities	Authorities responsible for carrying out checks on persons at external borders
Entry / Exit System (EES)	A system which registers entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Schengen States.[6]
European Travel Information and Authorisation System (ETIAS)	An automated online system for identifying irregular migration, security or public-health risks associated with visa-exempt TCNs travelling to the EU prior to their arrival[7], somewhat comparable to the American ESTA or Canadian ETA.
External borders	The parts of a Schengen Member State's border, including land borders, river and lake borders, sea borders and their airports, river ports, seaports and lake ports, that are not common borders with another Schengen Member State.
Extra-EU flight	Any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a EU Member State or flying from the territory of a EU Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries.
Extra-Schengen flight	Any scheduled or non-scheduled flight by an air carrier flying from outside the Schengen area and planned to land on Schengen area territory or flying from the territory of the Schengen area and planned to land outside the Schengen area, including in both cases flights with any stop-overs in the territory of the Schengen area or outside of it.
Extra-EU/Schengen flights	This term has been used in the document for any scheduled or non-scheduled flight by an air carrier flying from a third country planning to land in an EU Member State or on the Schengen area territory or flying from the territory of an EU Member State or the Schengen area and planned to land in a third country, including in both cases flights with any stop-overs in the territory of an EU Member State or the Schengen area or third countries.
Implementing countries	For the purposes of this evaluation, all 28 EU Member States (in 2019, i.e. the last year covered by this evaluation) plus the 3 Schengen associated countries implementing the API Directive (Switzerland, Iceland and Norway). Liechtenstein does not have an airport, therefore, even though bound by the Schengen acquis, was not included in this evaluation.
Internal Borders	Borders between Member States or Schengen associated countries
Interactive API System (i-API)	An electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities, who within existing business processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member.

[6] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32017R2226

[7] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584527668270&uri=CELEX:32018R1240

Interoperability	The ability of information systems to exchange data and enable sharing of information.
Intra-EU flight	Any scheduled or non-scheduled flight by an air carrier flying from the territory of an EU Member State planned to land on the territory of one or more of the Member States, without any stop-overs in the territory of a third country.
Intra-Schengen flight	Any scheduled or non-scheduled flight by an air carrier flying from one airport within the Schengen area planned to land at another airport within the Schengen area, without any stop-overs outside that area.
Intra-EU/Schengen flights	This term has been used in the document for any scheduled or non-scheduled flight by an air carrier flying from the territory of an EU Member State or the Schengen area territory planned to land on the territory of an EU Member State or the Schengen area, without any stop-overs in the territory of a third country.
Passenger	Any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person's registration in the passengers list.
Passenger Information Unit (PIU)	Units established or designated within the law enforcement authorities dealing with terrorist offences and serious crime at Member State level that collect, store and process PNR data.
Passenger Name Record (PNR)	A record of each passenger's travel details which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities. Air carriers shall transfer PNR data 24 to 48 hours before the scheduled flight departure time **and** immediately after flight closure (i.e. once passengers have boarded the aircraft). PNR data have to include API data if collected by the air carriers.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing of personal data	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Roll-out/Pilot	In the context of policy or practices, a test implementation of a programme, system or operational practice to assess whether it should be introduced more widely.
Schengen area	The Schengen area, i.e. the area without controls at internal

	borders, encompasses 22 EU Member States, all except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. Four countries that are not Member States. Iceland, Norway, Switzerland and Liechtenstein have joined the Schengen area (Schengen associated countries)**.**
Schengen associated countries	The countries which without being a Member State apply the Schengen acquis and have joined the Schengen area (Iceland, Norway, Switzerland and Liechtenstein).
Schengen Information System (SIS)	A joint information system that enables the relevant authorities in each EU Member State, by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks carried out within the Member State in accordance with national law and, for some specific categories of alerts, for the purposes of issuing visas, residence permits and the administration of legislation on aliens in the context of the application of the provisions of the Schengen Convention relating to the movement of persons.
Single Window	A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfil all regulatory requirements. If information is electronic then individual data elements should only be submitted once.
Stolen and Lost Travel Documents database (SLTD)	A database maintained by Interpol containing around 84 million records of lost, stolen and revoked travel documents, such as passports, identity cards, visas and UN laissez-passer, as well as stolen blank travel documents.
Systematic external border checks	Systematic checks refer to the practice of checking information on third-country nationals crossing the external Schengen borders against Interpol's Database of Lost and stolen travel documents (SLTD), national databases on lost and stolen documents and the SIS. Since April 2017, such checks have also become mandatory for EU citizens.
Targeting Centre	Capacity of Member States to conduct automated risk assessment of travellers based on the different travel intelligence (e.g. API, PNR, Visa Information System (VIS), EES, etc.) that can legally be used for border management and is based on tactical risk analysis. The aim is to detect unknown persons of interest (in comparison to known criminals on watch lists) before arrival at the border.
Third Country	For the purposes of this document, all countries that are not EU members nor Schengen associated countries.
Third Country National	Any person who is not a citizen of the European Union within the meaning of Art. 20(1) of TFEU and who is not a person enjoying the right of free movement under Union law, as defined in Art. 2(5) of Regulation (EU) 2016/399 (Schengen Borders Code).

Visa Information System (VIS)	System for the exchange of visa data between Schengen States, which enables authorised national authorities to enter and update visa data and to consult these data electronically.[8]

[8] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008R0767

1. INTRODUCTION

Purpose and scope

This evaluation assesses Council Directive 2004/82/EC of 29 April 2004[9] on the obligation of carriers to communicate passenger data (the 'API Directive') and its implementation in EU Member States and Schengen associated countries. The API Directive was adopted in 2004 with a transposition deadline of 5 September 2006 and was evaluated for the first time in 2012.[10] It aims at improving border controls and combating illegal immigration by the transmission of advance passenger information (API) by air carriers to competent national authorities. It also gives Member States the possibility to use the data for law enforcement purposes.

The key objective of the evaluation is to provide an understanding of whether the Directive's provisions are still 'fit-for-purpose' 15 years after its adoption and 7 years after its first evaluation. Hence, this document assesses whether and how the Directive still addresses the needs of border control authorities, law enforcement authorities, airline carriers, passengers and other relevant stakeholders, in the light of the recent developments at EU Level, such as the implementation of the passenger name record (PNR) Directive[11] and the expansion of the EU's large-scale databases and their interoperability, the increase of the number passengers travelling by air, the migratory pressure and renewed terrorist threats.

This evaluation is supported by an externally contracted study[12] (hereafter: "Evaluation Study"), as well as by meetings and workshops with stakeholders and experts. It assesses the effectiveness, efficiency, relevance, coherence and EU-added value of the Directive as follows:

- Material scope: current state of legal transposition of the API Directive; practical implementation of the API Directive; baseline assessment and evaluation based on the five evaluation criteria as per the Better Regulation Guidelines.
- Geographical scope: 31 countries (hereinafter: "implementing countries") – all 28 EU Member States[13] and the 3 Schengen associated countries implementing the Directive (Switzerland, Iceland and Norway). Liechtenstein does not have an airport, therefore, even though bound to the Schengen *acquis*, was not included in this evaluation.
- Temporal scope: 2012 to 2019 (period since the first evaluation).

---

9 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004L0082

10 Evaluation report available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/irregular-migration-return/return-readmission/docs/evaluation_of_the_api_directive_en.pdf

11 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 - https://eur-lex.europa.eu/eli/dir/2016/681/oj

12 Evaluation study available at: https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF/source-119728696

13 The United Kingdom left the European Union as of 1 February 2020. The reference period for this evaluation is 2012-2019, while the UK was a Member State. The study therefore includes information on the United Kingdom.

2. BACKGROUND TO THE INTERVENTION

Description of the intervention and its objectives

Advance Passenger Information (API) is commonly understood as the information of an air passenger collected at check-in or at the time of online check-in. API information includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight.

The API Directive is a 2004 Council Directive aiming at improving border controls and combating illegal immigration through the transmission of advance passenger data by carriers to the competent national authorities.

By means of its transposition into national law, the Directive imposes an obligation on air carriers to transmit, upon request, passenger data to the Member State of destination prior to the flight's take-off or shortly after take-off, if that flight is in-bound from a third country. It also gives to Member States the possibility of using API data for law enforcement purposes. The Directive was drafted with the spirit of 'minimum harmonisation', therefore it leaves to each implementing state the possibility to extend the obligations included in the Directive by means of national law[14].

The European Council Declaration on combating terrorism adopted in March 2004[15], in the aftermath of the terrorist attacks in Madrid on 11 March 2004, called for an early conclusion of the proposed Council Directive, put forward at the initiative of Spain, on the obligation of carriers to communicate passenger data. The Directive was adopted without the opinion of the European Parliament under "exceptional circumstances".

In light of the above, and in the absence of any Impact Assessment or preparatory document preceding the tabling of the proposal for the Directive, the intervention logic below provides an overview of the Directive's general and specific objectives and has been prepared by the contractor responsible for carrying out the external study. This tool serves to depict the chain of expected effects associated with the Directive.

The intervention logic identifies two general objectives pursued by the Directive. These are: 1) improving the management and protection of the EU external border while facilitating clearance of legitimate passengers and 2) enhancing security of EU citizens. The Contractor detailed these two general objectives into four specific points (called 'specific objectives'); two of them – improving border control and combatting illegal immigration - are referring to objectives explicitly listed in the text of the directive (art. 1). The other two points (law enforcement including in particular fighting terrorism) go beyond the objectives stated in the legal act but are linked with the Directive's provisions on ensuring security check at the borders and enabling implementing countries to use

[14] Recital (8) of the API Directive: "Without prejudice to the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the freedom of the Member States to retain or introduce additional obligations for air carriers or some categories of other carriers, including information or data in relation to return tickets, whether referred to in this Directive or not, should not be affected".

[15] https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf

API data for law enforcement purposes. In practice most Member Sates provided for such use of API data, which indicates the importance of this objective. It is also noted that recital 2, read in context of circumstances in which the Directive was brought forward by Member States, shows that fighting terrorism was one of the drivers for adopting the Directive.

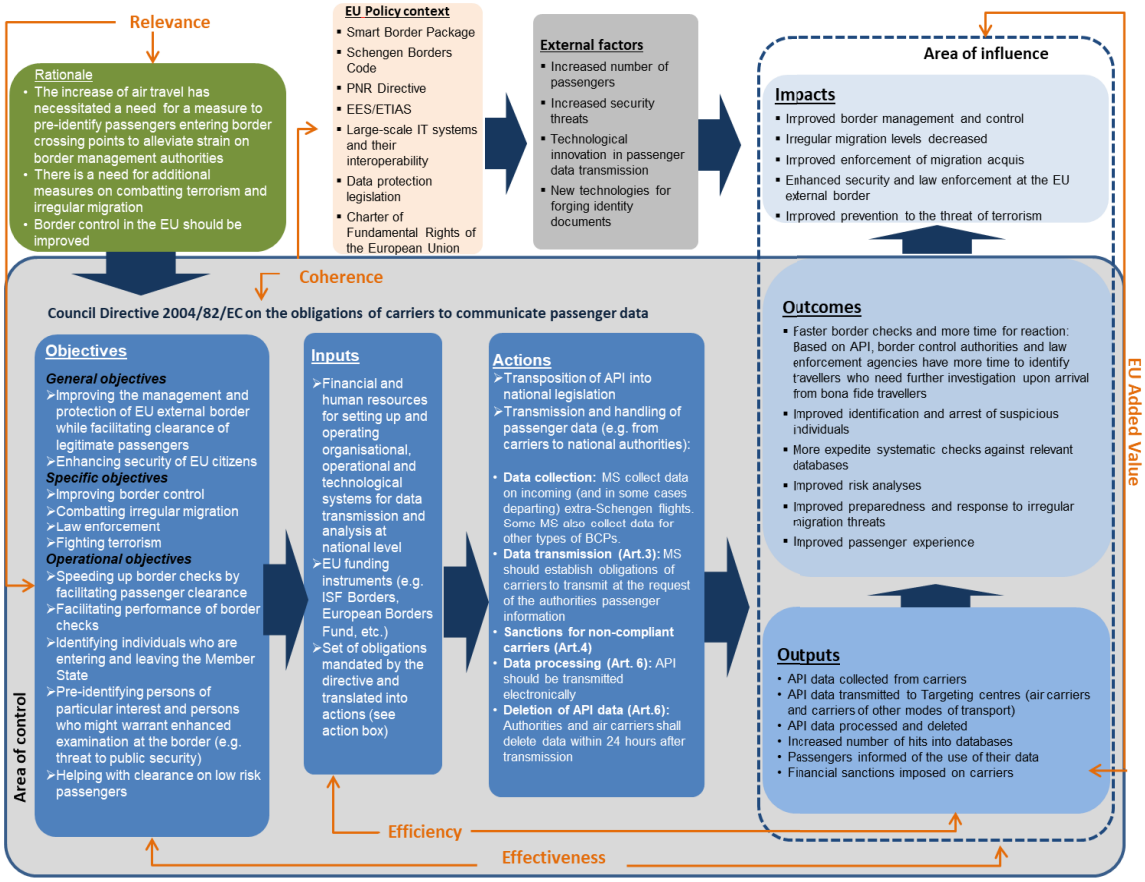


Figure 1 - intervention logic – Source : ICF – Evaluation Study

The intervention logic further identifies the following operational objectives:

1) Facilitating performance of border checks
2) Facilitating clearance of legitimate travellers
3) Identifying individuals entering the Member State
4) Pre-identify persons of particular interest and persons who might warrant enhanced examination at the border
5) Helping with clearance of low risk passengers

The intervention logic makes clear that where the outputs are met, the Directive should generate a number of outcomes that address the drivers that prompted the decision to take the initiative in the first place. The expected outcomes include: faster and more effective border checks, improved identification and arrest of suspected individuals, improved risk analysis. Assuming these outcomes are achieved, the Directive should ultimately lead to an improved level of border management and control, improved enforcement of migration acquis and enhanced security of the EU.

The intervention logic also identifies the external factors affecting the Directive including for example increases in the number of passengers; increased security threats and technological innovations and takes into account the policy context in which the Directive operates.

Baseline and points of comparison

The baseline of this evaluation is the situation as described in the study "Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82", carried out in 2012, which had *inter alia* highlighted the following elements:

- Most of the competent authorities considered that the objectives of their API system or legislation were fully in line with those of the Directive. Competent authorities also identified law enforcement as a perceived need at the time of transposing the Directive.
- The implementation of API systems has helped to improve border controls; for instance, through API systems, competent authorities have been able to:
    - Identify specific flights for which enhanced border checks are necessary (i.e. as compared to other flights) because the higher prevalence of non-EU nationals in those flights is known before landing;
    - Better preparation for the control of specific passengers by identifying them via API data in advance of their arrival; this helps to accelerate border checks because passengers requiring secondary checks can be separated from the other passengers and reallocated to separate lanes without the other passengers queuing and waiting;
    - Anticipate certain situations and the type of controls to be performed;
    - Check API data against other databases, and thus shorten the time for controls and checks at the external borders.
- Instances of late or partial implementation of API systems, or in some cases failure to implement API systems at all, were observed. In the countries implementing API systems in 2012, the systems' technical and operational capabilities varied, and the operational procedures underlying the API systems were inconsistent. This created some incoherence and uncertainty in the way in which API systems were operated.
- Possible issues of coherence in the future, with the adoption of other instruments (e.g. on PNR) were detected.

In order to facilitate the comparison between the baseline and the current situation, a brief summary of the 2012 state of play has been provided when assessing each evaluation criteria.

3. IMPLEMENTATION / STATE OF PLAY

The current regulatory landscape on API

At EU level, the API Directive regulates the collection and transmission of API data in all EU Member States[16] (including those Member States applying the Schengen acquis in

[16] The Protocol on the position of Denmark to the Treaty of Amsterdam, the Treaty on European Union and the Treaty establishing the European Community as amended by the Treaty of Lisbon, allows Denmark to decide whether or not it will participate (opt in) in measures building upon the Schengen acquis. Recital 13 of the API

full and those which do not yet apply the Schengen acquis in full, such as Bulgaria, Cyprus, Croatia and Romania) and Schengen associated countries (Norway, Iceland, Liechtenstein[17] and Switzerland). It places an obligation on air carriers to transmit, upon request, passenger data to the implementing country of destination prior to the flight's take-off or shortly after take-off, if that flight is in-bound from a third country. The primary objective of the Directive is to facilitate border control and to prevent irregular migration, but the Directive also recognises that API data can be used for law enforcement purposes, leaving to national legislation to regulate this use. The Directive only sets minimum standards for the implementing countries to request API data and implementing countries are free to request similar data from other transport carriers, such as maritime or rail transport carriers.

At international level, Annex 9 of the Convention on International Civil Aviation (Chicago Convention)[18] as well as the WCO[19]/IATA[20]/ICAO[21] API Guidelines[22] are the main international regulatory instruments on API. Besides, UN Security Council Resolutions 2178(2014)[23], 2309(2016)[24], 2396(2017)[25] and 2482 (2019)[26] call upon UN Member States to require airlines operating in their territories to transfer API to national authorities to detect departures or attempted entry or transit of suspects with the aim to counter terrorism. Since February 2018, the establishment of national API systems is an ICAO standard, making it mandatory for all Contracting States to the Chicago Convention.[27] In addition, the OSCE[28] Ministerial Council has adopted, on 8 December 2016, a Decision on enhancing the use of API, whereby OSCE participating States commit, *inter alia,* to establishing a national API system.

At EU level, in addition to the API Directive, Directive 2016/681 on the use of Passenger Name Record (PNR) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[29] was adopted in 2016 (hereafter: the PNR Directive). The PNR Directive requires air carriers to transfer PNR data collected in the normal course of their business to the Member States' Passenger Information Units (PIUs). Annex I of the PNR Directive includes API[30] among the data to be transferred by carriers

---

Directive recalls this and states that Denmark 'shall decide within a period of six months after the Council has adopted this Directive whether it will implement it in its national law'. Accordingly, Denmark notified the Commission of its willingness to participate in the implementation of the API Directive in 2006. However, this participation entails no obligation under EU law, but rather sets up a relationship based on International Public Law rules. Hence, Denmark is not bound to transpose the provisions of the Directive, but rather to implement them.

17 Liechtenstein does not have an airport, therefore, even though bound to the Schengen acquis, was not included in this evaluation.

18 ICAO Convention on International Civil Aviation, available at: https://www.icao.int/publications/pages/doc7300.aspx

19 World Customs Organization - http://www.wcoomd.org/en.aspx

20 International Air Transport Association - https://www.iata.org/

21 International Civil Aviation Organization - https://www.icao.int/Pages/default.aspx

22 WCO/IATA/ICAO Guidelines on Advance Passenger Information, available at: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/api-guidelines-main-text_2014.pdf

23 UN Security Council Resolution 2178(2014) https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29

24 UN Security Council Resolution 2309(2016) https://undocs.org/S/RES/2309(2016)

25 UN Security Council Resolution 2396(2017) https://undocs.org/en/S/RES/2396(2017)

26 UN Security Council Resolution 2482 (2019) http://unscr.com/en/resolutions/doc/2482

27 Annex 9 to the convention on International Civil Aviation.

28 Organization for Security and Co-operation in Europe - https://www.osce.org/

29 https://eur-lex.europa.eu/eli/dir/2016/681/oj

30 Type, number, country of issuance and expiry date of any id document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time.

as far as collected for their own business purposes. The PNR Directive also requires Member States to adopt the necessary measures to ensure that carriers transfer any available API data collected in the course of their business, to the PIU, in which case "the provisions of the PNR Directive shall apply to those API data" (Article 8(2)).

The transposition of the API Directive

The API Directive was transposed at different paces in different Member States.

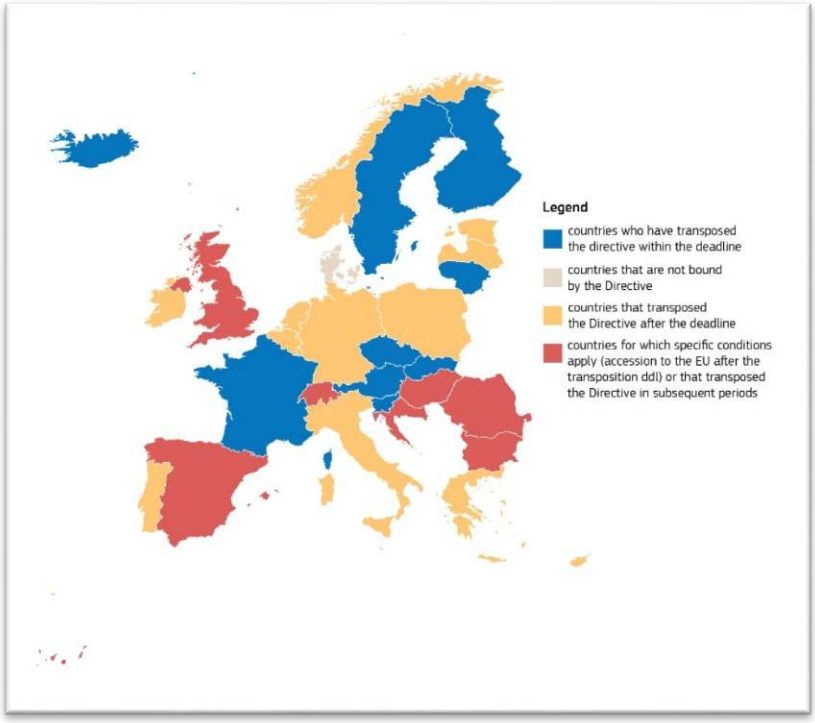


Figure 2- transposition of the API Directive

While today all implementing countries have transposed the Directive, as shown in figure 2, only 9 countries had transposed the Directive within the deadline of 5 September 2006.

It should be noted that many implementing countries, despite having transposed the Directive, did not have an API system in place for many years; in fact the Directive does not impose on implementing countries an obligation to request any data. It only requires airlines to collect and transmit the data upon request of the implementing country.

Overall, the API Directive was adequately transposed. Article 1 on the objectives and Article 6 on data processing contain provisions that triggered most cases of incorrect or incomplete transposition or transposition going beyond the Directive's provision.

Article 1 sets out the twofold objective of the API Directive, namely, 1) combating irregular migration, 2) improving border control. Half of the implementing countries have nonetheless adopted an implementing approach that goes beyond those two requirements.

Firstly, five implementing countries have enshrined the fight against terrorism as an objective of their API system.[31] The API Directive allows for the use of API data for law enforcement purposes. Recital (2) of the Directive also makes a reference to a Council Declaration on terrorism adopted following the Madrid terrorist attacks. Secondly, several countries have made use of the possibility offered by Article 6(1) subpara 5 to collect API data for law enforcement purposes[32]. This is for example the case of Cyprus, where API data may also be used to investigate offences leading to an imprisonment sentence of 1 year or more (3 years or more in Slovakia), and in Austria, where API data can be transmitted to another law enforcement authority in case of suspicion of a criminal offense. Slovenia has recently opted for this legal choice (2017) and is currently amending its related laws. In the United Kingdom, the national transposing regulation goes beyond the objectives of the API Directive by including law enforcement and intelligence as one of the ultimate goals. Figure 4 below (found on p.13) provides an overview of the practical implementation and purposes for the use of API data.

Article 6 emerged as the most problematic provision of the API Directive in terms of transposition into the national legal frameworks. This provision sets out the rules applicable to the processing of the API data collected. Due to the references made to data protection rules, this provision is particularly important but also complex to implement. For the sake of clarity, the analysis of the compliance of national legislations with data retention requirements is presented separately (see page 19: "Transposition and implementation - a data protection perspective").

The implementation of the API Directive

In recent years, the implementation of the PNR Directive, together with the international commitments made by contracting states in ICAO and OSCE, have given a strong impetus to the use of API data in the EU.

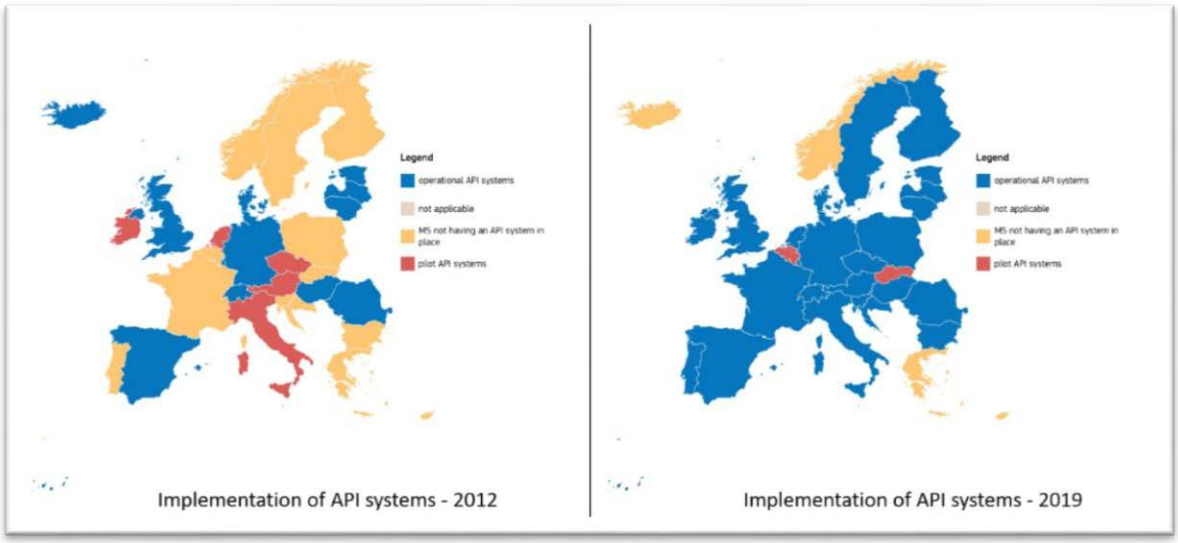


Figure 3– implementation of API systems in 2012 and in 2019

[31] BE, FR, HR, LT and CH.
[32] AT, BG, CY, DE, DK, EE, EL, ES, LV, SI, and SK.

As shown in Figure 3 above, in 2012, 18 out of 30 implementing countries[33] had API systems in place (only pilots in some cases), in 2019, 25 out of the 31 implementing countries had fully functioning API systems in place. Two implementing countries still were running pilot systems (Belgium and Slovakia) and four implementing countries (Cyprus, Greece, Iceland, Norway) did not have an API system but were planning to establish one post 2019. Liechtenstein did not have an API system in place and does not plan on setting one up as it does not have an airport. Therefore, it is not included among the "implementing countries", despite being a Schengen associated country.

Purpose

As regards to the purposes of API data collection, based on the interviews carried out during the Evaluation Study, 29 implementing countries collect (or are planning to collect) API data with the aim of combatting irregular migration; 29 implementing countries for the purpose of improving border control; 21 implementing countries for law enforcement purposes and 15 for fighting against terrorism.[34]

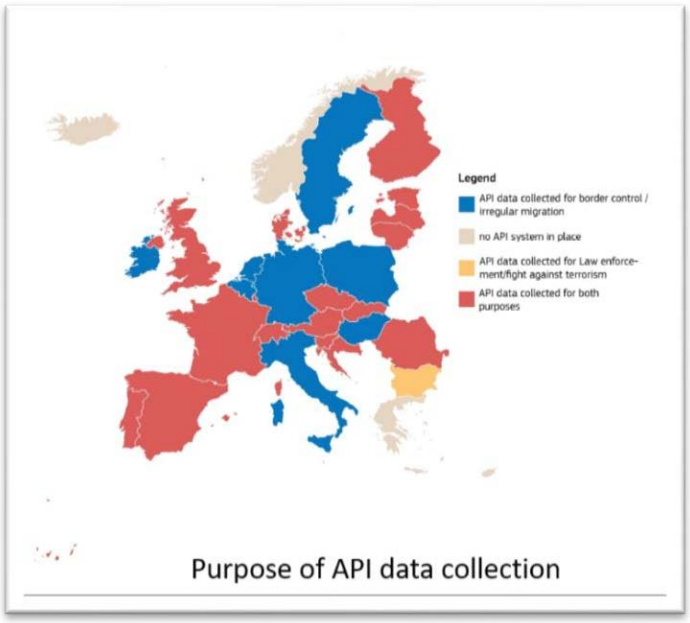


Figure 4 – purpose of data collection

Scope

Concerning the scope of API data collection, i.e. the type of flights and the type of carriers covered, the API Directive gives flexibility to implementing countries to limit the API data collection to certain airports, flights and carriers. Regarding the airports, 22 implementing countries[35] out of the 31 consulted (74%) collected API data for all relevant airports, i.e. airports with extra-EU/Schengen flights, while four[36] did not collect API data for all airports handling such flights. The rationale for limited coverage ranged

[33] "30 implementing countries" refers to all 31 implementing countries, minus Croatia as in 2012 it was not an EU Member State.

[34] Despite the fact that terrorism is actually part of law enforcement, implementing countries were asked both if they use API data for law enforcement and for fighting terrorism, leading to presenting the two issues separately.

[35] AT, BG, CZ, DE, DK, EE, ES, HR, IT, FR, FI, LT, LV, LU, MT, NL PT, PL SE, SI, RO, UK.

[36] CH, HU, IE, SK. In Hungary, Only at three biggest airports: Budapest, Debrecen and Sármellék. In practice, all other airports in Hungary have negligible traffic.

from the relatively small size of the airports, low volume of international air traffic, location (only capital cities covered) and airports with low-risk routes according to border control authorities' analysis.

Regarding the flights covered, the majority of implementing countries[37] receive or are planning to receive API data for all inbound extra-EU/Schengen flights to their territory, while seven implementing countries[38] collect or are planning to collect data only on selected flights. Flights for which data are not typically collected include charter flights. The rationale for only selecting certain flights is based on risk analysis usually involving the border control and migration authorities. In Germany, for example, risk routes are flights departing in a country or airport that has been identified by the border control authority as posing a certain risks, e.g. in relation to terrorism or irregular migration.

Article 3(1) of API Directive limits its scope to inbound flights from third countries. However, several implementing countries request API data also for other flights: twelve implementing countries[39] request data for outbound flights and eight implementing countries[40] for intra-EU/Schengen flights. Three implementing countries reported requesting API data for domestic flights[41]. The collection of API information on outbound extra-EU/Schengen flights and on intra-EU/Schengen flights is linked to the scope of the PNR Directive. Under Article 2(1) of the PNR Directive, EU Member States may decide to apply the Directive also to intra-EU flights. Currently, 24 EU Member States have both fully transposed the PNR Directive and communicated to the Commission that they intend to apply it to intra-EU flights.[42] Implementing countries which collected API data on intra-EU flights did so based on the PNR Directive and for law enforcement purposes, and only where air carriers collect the data in the normal course of their business.

Out of four implementing countries that do not yet apply the Schengen acquis in full (Bulgaria, Croatia, Cyprus and Romania)[43], only Bulgaria reported to request API data on intra-EU flights from air carriers and confirmed to apply the provisions of the API Directive to these flights.

As for the scope of the API data collection in terms of air carriers, API data is being requested (or planning to be requested) from all air carriers[44] in 19 countries[45] whilst in 12 implementing countries[46] it is requested for selected air carriers only.

In some implementing countries, API data collection has also been mandated for other modes of transport – i.e. in ten implementing countries API is being collected from waterborne carriers; in four from trains and in one from coaches/buses.

---

37 AT, BG, CZ, EE, ES, FI, HR, HU, IE, IT, LT, LV, MT, NL, PT, RO, SE, SI, SK* UK, IS* (*planned).
38 CH, DE, DK, FR, LU, NO*, PL.
39 BE, BG, DK, EE, FI, FR, LT, PL, RO, SI, SK, UK.
40 BG, DK, FR, LT, SI, SK, UK, IS.
41 BG, DK, FR (only for flights from French overseas territory).
42 https://ec.europa.eu/home-affairs/news/list-member-states-applying-pnr-directive-intra-eu-flights_en
43 In addition to these four Member States which do not yet **fully** apply the Schengen acquis, Ireland and the United Kingdom are not part of the Schengen area.
44 This only refers to "scheduled flights" i.e. it does not concern charter flights and business aviation.
45 AT, BG, CY*, CZ, DK, EL*, ES, FR, HU, IE, LT, LV, SE, SI, UK, FI, IS*, LU, MT.
46 BE, CH, EE, HR, NL, PL, SK, IT PT, RO, NO*, DE.

Modes of transport	Member States
Air carriers	AT, BG, CH, CZ, DK, EE, EL*, ES, FR, HR, HU, IE, LT, LV, MT, NL, PL, PT, SE, SI, SK, UK, RO, IT, NO*, FI*, ISL*, DE, CY*, LU
Waterborne carriers	AT, BE*, EE, ES, FR, HU, MT, UK, NO*, FI, ISL*
Trains	EE, FR, FI, UK
Coaches/buses	AT

*Figure 5- API collected per mode of transport. *Planned. Source: ICF – Evaluation Study*

Data fields

Looking at the data fields, Article 3(2) of the API Directive provides for a list of API passenger data (number and type of travel document, nationality, full names, and date of birth) and flight data (border crossing point of entry, code of transport, departure and arrival time, total number of passengers carried and initial point of embarkation). The list is non-exhaustive and implementing countries can request additional data elements in line with national legislation. API data is also included under point 18 of Annex I of the PNR Directive which lists API data elements additional to those listed in Art.3(2) of the API Directive, which include gender, departure and arrival date of transportation, name of the airline, flight number, country of issuance and expiry date of the travel document.

All implementing countries request the full names of the passenger. With the exception of Iceland, all implementing countries require the travel document number, document type, nationality, date of birth (DOB) and arrival time. With the exception of Estonia, all implementing countries request data concerning the departure time. In addition to the data fields provided in the API Directive, 24 request additional data elements. Most common additional data fields include country of issuance of the travel document, gender, flight number and airline, with a range from 14 to 24 implementing countries. Other less commonly reported data fields include expiry date of travel document (9 instances)[47], points of transit (4)[48], seat and baggage information (4)[49], dates of departure and arrival (3)[50], crew data (2)[51], place of birth(1)[52] and duration of flight (1)[53]. Four (4) countries[54] suggested adding visa number to the API data list to avoid ambiguous situations when travel documents with different numbers have been used. Currently, visa number is used by one (1) Member State.[55] Other Member States suggested collecting additional data elements, such as: information on the person's entire journey[56] and ticket information.[57]

47 BE, CH, DK, EL, FR, LT, MT, NL, UK.
48 BE, CH, HU, DE.
49 BE, FR, SI, NO (requested only *ad hoc*, based on risk assessment).
50 BE, BG, NL, UK.
51 BG, ES, NL.
52 IT.
53 IT.
54 AT, CZ, DK, LV.
55 LT.
56 EE, LT, DE.
57 EE: This information is collected with the PNR, but the border control unit does not receive that information. This information could be an extra piece to help the border guard to assess the real purpose of the travel.

Gender, issuing state or organisation of the official travel document and expiration date of the validity of the official travel document[58] are amongst the data elements not mentioned in the API Directive but contained in the MRZ. Relevant EU instruments[59] and internationally recognised standards,[60] recommend including MRZ data fields in the instrument governing the API data collection and processing. Doing so would increase the quality of the data captured. Finally, data elements such as seat and baggage information are seen as essential for advance screening of passengers by some of the Member States, and are already part of a standard WCO/IATA/ICAO Passenger List Message (PAXLST)[61], a data format used by carriers to transfer API data when transferred separately from the PNR message.

Organisational set-up and governance

The main authorities involved in the implementation of API systems include Border Management Authorities, Ministries of Interior and Data Protection Authorities; the main organisational focal points which collect and/or process API are 'single window', 'Passenger Information Units' and 'Targeting Centres', described below.

In terms of receiving API data by national authorities, international standards prescribe the 'single window' approach. According to ICAO[62], the single window concept should apply to each form of passenger data that an airline is obliged to transmit to the requesting authority, i.e. Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR). Implementing countries should designate an authority to receive all forms of passenger data in one single entry point and then distribute this data to all those national authorities with the legal remit to receive and use this data. This is expected to increase effectiveness not only in terms of border security, but also alleviate duplicative costs for the airline industry as well as each individual agency that might have legal authority to view the data. Nearly half of the implementing countries (13)[63] use the single window model.

Nearly half of the implementing countries (14)[64] reported that they processed API data together with PNR data[65] (mainly API data collected as per the provisions of the PNR Directive). In accordance with Art. 4(1) of the PNR Directive, Member States shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its passenger information unit ('PIU'). The PIU may, however, have different branches in one Member State and Member States may also establish one PIU jointly.

---

58 WCO/IATA/ICAO Guidelines on Advance Passenger Information, version 2013, available at: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx

59 While Article 45(2) of ETIAS Regulation refers to MRZ data as part of carriers' interactive query, Article 13(3) of EES Regulation specifies the individual components, corresponding to the MRZ.

60 Annex 9 to the Convention on International Civil Aviation, Fifteenth edition, October 2017.

61 Appendix IIA to Advance Passenger Information Guidelines, WCO/IATA/ICAO Passenger List Message (PAXLST) Implementation Guide, October 2013, Version 3.0, available at: https://www.icao.int/Security/FAL/Documents/3.API%20Guidelines%202013%20Appendix%20II%20A%20-%20PAXLST%20Message%20Implementation%20Guide_English_Only%20updated.pdf

62 Recommended Practice 9.1— https://www.icao.int/Meetings/FALP/Documents/FALP9-2016/FALP9_WP9_Single-Window-Concept_IATA.pdf

63 BE, BG, CZ, DK, FR, HU, LT, MT, SE, SI, SK, UK, NO (planned for summer 2020).

64 BE, BG, DK, EE, FR, HU, IE, LT, LU, MT, SE, SI, SK, UK.

65 Whilst in most Member State this refers mainly to API data collected as per the provisions of the PNR Directive, in some of these 14 Member States it was not specified if the API data was collected on the basis of the API Directive or the PNR Directive.

The remaining implementing countries[66] answered negatively as to the common processing of API/PNR data.

A key question is whether implementing countries have established Targeting Centres for processing API data. A 'Targeting Centre' is understood as the capacity for implementing countries to conduct automated risk assessment of travellers based on the different travel intelligence collected (e.g. API, SIS, VIS, EES, etc.) that can legally be used for border management and based on tactical risk analysis[67]. The aim is to detect unknown persons of interest (in comparison to known criminals on watch lists) before they come to the border.[68] Such capacities are already functioning in a few third countries, such as the United States and Canada, but there are few of these capacities in the European Union, the oldest being the National Border Targeting Centre (NBTC) in the United Kingdom.

At present, thirteen implementing countries[69] have set up Targeting Centres (although the set-up of these Targeting Centres varies across countries), whilst eighteen countries do not have a functioning Targeting Centre. In implementing countries which have set up Targeting Centres, this role is typically carried out by the 'Passenger Information Units' (PIUs).

Across implementing countries, there is quite a variety of organisational structures. For example, in Ireland, the PIU is the targeting centre and receives, processes and analyses both the API and PNR data. While the API data is normally checked against the migration related databases, the PNR data is being checked for terrorism and serious crime related threats. Another example is the Netherlands, where API and PNR are processed separately by different authorities – i.e. API Centre and PIU (Pi-NL). API data is processed by the Border Authorities which fall under the Ministry of Defence, PNR data is processed by PIU (Pi-NL), which is an independent unit hosted by the Ministry of Defence, but falls under the responsibility of the National Coordinator for security and counter-terrorism.

Sanctions

Article 4 of the API Directive provides that implementing countries shall impose sanctions to carriers and indicates that either the maximum amount of such sanctions should be not less than EUR 5 000; or the minimum amount not less than EUR 3 000. In addition to financial sanctions, the Directive provides that implementing countries can impose other types of sanctions for carriers which infringe very seriously the obligations arising from the provisions of this Directive. These sanctions are immobilisation, seizure and confiscation of the means of transport, or temporary suspension or withdrawal of the operating licence.

Implementing countries indicated that occasionally they have issues with accuracy or completeness of data transmitted by carriers. There have been two general approaches to managing air carriers in regard to transmission of API data: (1) engaging with carriers without resorting to sanctioning and enforcement actions, and (2) more straightforward approach to aggressive enforcement sanctioning non-compliance. In both cases, the

66 AT, CH, CZ, ES, HR, FI, IS*, DE, LV, NL, PL, PT, RO, IT, NO* - In addition, Cyprus and Greece do not have an API system and have not responded to this question. (*planned).
67 European Border and Coast Guard Agency (2018), Report on API systems and Targeting Centres.
68 Ibid.
69 BE*, BG, DK, ES, FR, HU, IE, LT, MT, NL, SI, SK, UK (*planned).

statistical information presented by implementing countries indicates that the rates of incorrect data transmission, as well as the instances of incorrect or incomplete data have been declining over time.

Seventeen implementing countries[70] out of the examined thirty-one, have not imposed any sanctions to carriers, while, in fourteen countries[71], fines have been imposed for the violation of obligations related to the transmission of API data.

The absence of sanctions imposed seems to be the consequence of effective coordination between airlines and national authorities receiving the data. In this sense, as soon as the authorities observe any lacks/defects/invalidate data, they directly contact the relevant airline to get clarity or to collect the proper data. As a result, most defects are solved directly without restoring to sanctions.

This approach is also in line with Annex 9 to the Convention on International Civil Aviation, whereby the Contracting States 'should refrain from imposing fines and penalties on aircraft operators for any errors caused by a systems failure' in transmitting API data to authorities. Rather than imposing sanctions, Annex 9 foresees mitigation measures and necessary system maintenance to be undertaken in case of such failure. More specifically, Annex 9 states that the Contracting States and aircraft operators should provide operational and technical support to analyse and respond to any system outage or failure continuously. Also, the document calls for implementing appropriate notification and recovery procedures for both planned and unexpected system outages.

Out of the 28 carriers which responded to the industry survey, 10 have been sanctioned by implementing countries. Consulted air carrier representatives feel that some implementing countries are not always working in partnership with carriers – e.g. authorities might fine the airline without prior notice when the airline is not even aware that there is a problem with the data. Moreover, sanctions are often seen as too severe and inconsistent between countries.

Transposition and implementation - a data protection perspective

When describing the implementation of the API Directive, particular attention should be given to whether the practical implementation is in line with the data protection requirements put forward by the Directive[72] and the applicable EU and national data protection legislation. The 2012 evaluation already showed that ten implementing countries allowed the authorities to store the data for longer than 24 hours. None of them, except one, mentions that the data can be kept for longer than 24 hours only for 'statutory purposes'.[73] Even more, Member States which keep data beyond the deadlines provided

[70] BE, BG, DK, EE, EL, FR, IE, LU, NL, PT, SE, SI, SK, UK, CY, NO, IS.

[71] AT, CZ, ES, HU, HR, IT, FI, DE, LV, LT, MT, PL, RO, CH.

[72] The main data protection elements included in the Directive are: 1) the obligation for the authorities to save the collected data in a temporary file (Article 6 (1), par. 2); 2) the obligation for the authorities to delete the data within 24 hours after transmission unless the data are needed for exercising their statutory functions in accordance with national law and subject to data protection provisions under Directive 95/46/EC (Article 6(1) par.3); 3) the obligation for carriers to delete data within 24 hours of the arrival of the means of transport (Article 6(1) par.4); and the obligation for carriers to inform the passengers in accordance with the provisions laid down by the Data Protection Directive, and in particular, in accordance with Articles 10 (c) and 11(c). (Article 6(2)).

[73] See API directive, art. 6.1 "After passengers have entered, these authorities shall delete the data, within 24 hours after transmission, unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive 95/46/EC".

in the Directive, do not apply appropriate safeguards. Only one implementing country anonymised API data when retained for longer than 24 hours, while many implementing countries restricted access to API data by making use of data security tools. Furthermore, in 2012, only a few of the implementing countries with an operational API system had implemented systematic monitoring of compliance of national API systems with data protection standards and API systems were rarely inspected by data protection authorities.

The current state of play of the transposition and implementation of the API Directive shows that the API data collection pursue multiple objectives in several implementing countries. The variety of purposes for collecting data inevitably adds complexity to ensuring compliance with the data protection framework. Indeed, while most implementing countries transposed the obligation to transmit data to competent authorities as prescribed by the API Directive, there are significant differences in the organisational structures established to collect API data, as well as a variety of processes used for the collection and transmission of data. The implementation of API systems showed that, depending on the 'model' set up by implementing countries, authorities which receive, process and analyse API data vary greatly. In most implementing countries, border control authorities are the main authorities receiving data and having direct access to data. Other authorities (law enforcement authorities) have indirect access and need to justify the need for accessing the data. In this context, a few implementing countries do not receive data in an electronic format which, from a data protection perspective, represents a challenge as to how to efficiently ensure the restrictions regarding access to data and traceability of accesses and transmissions to other authorities.

In implementing countries adopting a 'single window' model and where the PIU acts as the targeting centre, data protection standards follow the PNR Directive, as the PIU's Data Protection Officer is in charge of ensuring that API data is received and accessed by other national authorities following the relevant data protection requirements (e.g. keeping an access log). In this context, border authorities receive API data indirectly and their processing of API data generally respects the limit of 24 hours set in the API Directive.

However, the implementation of the requirement to delete API data within 24 hours was problematic in several implementing countries, because of faulty transposition of this obligation in the national legislation, or because of overlaps with obligations coming from the PNR Directive, or both elements at the same time. As a result, in a few implementing countries, the 24 hour limitation set out in the API Directive was deleted from national legislation, which creates either a legal grey area as to which retention requirements should be applicable and/or leads to the sole application of the requirements set in the PNR Directive, despite the fact that API data and PNR data are different sets of data. Additionally, implementing countries have generally made use of the possibility included in the API Directive to store API data for longer than 24 hours where this is necessary for the exercise of "statutory functions". Most implementing countries have not defined a time limit in this case.

Passengers are informed of their rights by air carriers generally at the time of booking and/or via data privacy notices on their websites. The completeness of information varies from air carrier to air carrier. Generally, national air carriers provide more extensive information on data protection rights.

As in the 2012 evaluation, the monitoring of the compliance of API systems with data protection requirements was not systematic.

4. METHOD

Short description of methodology

Most of the methodological steps of this evaluation were carried out with the support of an external contractor who reported on their findings and recommendations in their study on evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 – Final Report, March 2020. The results of the report were discussed and analysed by the API evaluation Inter-Service Steering Group and lead to the conclusions highlighted in this paper.

The methodology consisted of the following steps:

1) **Inception:** ensure understanding between the external contractor and the Inter-Service Steering Group, agree on objectives and timing, carry out initial desk review and consultations, develop data collection tools and risk mitigation strategy.
2) **Data collection and stakeholder consultations**[74]: establish the baseline of the analysis, carry out national research, desk research, stakeholder consultations (including Public Consultation) and industry e-survey.
3) **Analysis**: assess and compile the results of research, surveys and consultations, evaluate and assess findings and discuss them at an expert workshop.
4) **Synthesis: conclude on the results of the evaluation study, considering other inputs coming from stakeholders, and develop conclusions on each evaluation criterion.**

Throughout all the steps, a range of methodological tools and techniques were used. These included: more than 30 interviews; targeted consultations with different stakeholders using online surveys and one workshops involving various experts; in addition, the Commission conducted a public consultation the results of which were made available to the contractor carrying out the external study.

A wide range of stakeholders were consulted as part of the evaluation. These included: national authorities; carriers and industry; technological providers, NGOs and EU Agencies. A more detailed description of the consultations is described in the Synopsis Report in Annex II.

A more elaborate description of the methodologies applied and the stakeholder consultations are provided in Annexes II and III.

Deviations from the Evaluation Roadmap

While the Evaluation Roadmap that was published in December 2018 indicated that the evaluation should have been completed in the last quarter of 2019, the actual completion date was in the second quarter of 2020. This was due to the fact that the public consultation was launched later than initially anticipated. In order to allow enough time

[74] More details on data collection methods, data analysis, consultation modalities, etc. can be found in annex 2 and 3 to this document.

to process and analyse the outcomes, the Commission opted to extend the evaluation timeframe into 2020.

Limitations and robustness of findings

The main limitations encountered during this evaluation were the following:

1) Limited literature and "evaluative" evidence (i.e. evidence on what works well, desirable outcomes, etc.)
2) Unavailability of documents related to the preparation of the legislative proposal (the Directive was adopted in 2004 - pre-Lisbon Treaty and with no opinion from the European Parliament or an impact assessment)
3) Quantitative data (such as on number of hits[75]) and budgetary data not readily available in implementing countries
4) Limited responsiveness of some stakeholders

This was mitigated as follows:

1) Comprehensive primary data collection and analysis compensated for the lack of a substantial body of literature
2) Support via Permanent Representations to facilitate contacts with stakeholders in implementing countries
3) Where quantitative data was not available, alternative proxy data or qualitative evidence was provided in the analysis
4) Approximations and assumptions where data was not available have been clearly outlined.

Despite the above, the findings of this evaluation picture clearly the current situation with regards to the use of API Directive. A general caveat: issues as "secure borders" or "accuracy of border checks", or even the costs for a public administration to run a border check, can often only be estimated and might depend on perception. In its evaluation report, the contractor made sure to refer to opinions every time hard data was not available, and the same is done in this report.

5. ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS

This evaluation builds on the study "Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data"[76] and it assesses the directive according to five criteria listed and described below. More information on each criterion, as well as on the source of each piece of information, can be found in the study itself. The evidence gathered in the study has been reviewed and analysed together with other sources of data in order to complete the picture for each criteria and to give a definite answer to each evaluation question.

[75] "Hit": an instance of finding or matching particular data in a computer search.
[76] https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF/source-119728696

5.1. RELEVANCE

The main question addressed in this paragraph is whether the objectives of the API Directive are pertinent to the needs of the stakeholders, and to which extent the intended benefits respond to problems and issues. This paragraph also looks at how well the Directive is adapted to future economic, technological, scientific, social, political and/or environmental advances.

2012 baseline situation on relevance

- In 2012, the Directive was assessed against the needs related to combatting irregular migration and improving border control, which are the two objectives defined in art. 1. More specifically, in relation to combating irregular migration, implementing countries highlighted the need of identifying persons banned from entering Schengen, identifying persons destroying their travel documents mid-flight in order to subsequently claim asylum, identifying document forgeries, etc. With regard to border control, implementing countries mentioned specific national needs, such as ensuring a smooth traffic flow at the air border crossing points, implementing a 'Smart Border' system, enhancing passenger experience, receiving information before the border crossing points in order to enhance the preparedness of border checks, etc.
- Implementing countries' competent authorities with a longstanding tradition of fighting against terrorism also identified law enforcement as a perceived need at the time of transposing the Directive.
- The perceived national needs at the time of transposition largely align with the objectives of the Directive. Almost all implementing countries recognised the objectives of the Directive as relevant to national needs at the time of transposition, which also matched to the current national needs as identified by national stakeholders. Yet for a few implementing countries, one of the main reasons for transposing and / or implementing the Directive was to comply with the Immigration and Asylum acquis as part of accession to the Schengen area with no particular national needs, problems or issues identified a priori.

2019 key findings on relevance

- The rationale for collecting API data is still valid across all stakeholders.
- The objectives of the API Directive listed in the text of the Directive (improving border control and combating irregular immigration) remain highly pertinent to the needs of the relevant stakeholders, as confirmed by the vast majority of consulted stakeholders across different stakeholder groups.
- Law enforcement including the fight against terrorism (identified as 'specific objectives' under the intervention logic) also remain, in the view of the stakeholders, highly pertinent to their needs.
- Amongst the main external factors driving the need for collecting API are the increase of passenger flows as well as the level of professionalisation and internationalisation of criminal groups and their cross-border activities. These factors are both likely to keep playing a role in the future.
- Collecting API data is also relevant to facilitate legitimate travel which is currently not per se an objective of the Directive.

The objectives[77] of the API Directive remain highly pertinent to the needs of the relevant stakeholders, as confirmed by the vast majority of consulted stakeholders across different stakeholder groups. Interviewed implementing countries' competent authorities[78] confirmed that the needs and problems tackled by collecting API data relate precisely to the objectives identified in the API Directive, i.e. border control management, combating against irregular migration, law enforcement including the fight against terrorism.

This is also corroborated with the responses to the Public Consultation:

- 85% of respondents strongly agreed or agreed that the API Directive is relevant to enhancing internal security;
- 83% of respondents strongly agreed or agreed that the API Directive is relevant to improving border control;
- 78% of respondents strongly agreed or agreed that the API Directive is relevant to fighting crime such as terrorism;
- 75% of the respondents strongly agreed or agreed that the API Directive is relevant for combatting irregular migration

In addition, according to stakeholders, the use of API data can contribute to speed up border checks, and as such is considered a useful travel facilitation tool, in particular in light of the increase of air travel and the growth of the number of passengers. In recent years, the number of passengers in air travel has increased significantly in all regions of the world. In the last 6 years, the total number of air passengers taking off or landing in the European Union has increased by over 25% - i.e. from 830 million in 2012 to over 1 billion in 2017 – with around 40% of those passengers being international extra-EU passengers.[79] Although the COVID-19 crisis, which emerged outside of the temporal scope of this evaluation, is having a substantial impact on the volume of travellers, a recent survey[80] of commercial airlines worldwide, indicates that the majority of respondents expect flights activities to recover within 2 years, thus suggesting a likely continuation of the long-term trend in passenger growth.

[77] As illustrated in the intervention logic, within the general objectives of improving the management and protection of EU external borders and enhancing security, four specific objectives of the API Directive were identified, namely (i) improving border control; (ii) combating irregular immigration; (iii) law enforcement (enhancing internal security and public order) including in particular (iv) fight against terrorism.

[78] Border Management Authorities, Ministries of Interior/Justice and PIUs and Targeting Centres.

[79] Eurostat [avia_paoc].

[80] Source: ICF: https://www.icf.com/insights/transportation/covid-19-commercial-aviation-impact.

Stakeholder	Potential (expected) benefits of API
Passengers	• Reduce waiting times for passenger clearance upon arrival
Carriers	• Enhance carrier security • Ensure that all passengers carry valid official travel documents required for admission to the destination country • Reduce carrier exposure to penalties for transporting passengers that are not properly documented • In case of interactive API, carriers are able to provide "Board/ Do Not Board" responses at time of check-in and be able to avoid costs associated with the detention and/or removal of persons who might otherwise be determined to be inadmissible upon arrival at the final destination.
National Authorities	• Advance screening of passengers and identification of those passengers that present risk • Enhance enforcement capabilities against inadmissible persons • Provide faster clearance of low risk passengers • Facilitate the flow of low-risk passengers at airports • Ensure a more effective allocation of border control and law enforcement resources and reduce staff costs
Societal benefits	• Better protection of EU citizens • Higher security and reduced cross-border crime • Facilitated flow of passengers at air borders
Other benefits	• Assist the growth in passenger traffic being accommodated through improved use of technology rather than additional infrastructure • Greater passenger satisfaction with facilities, fewer complaints • Better public image nationally/internationally, good for tourism (for example in preventing queues at arrival and or improving waiting times at the border)

Table 1 : Benefits of collecting API per stakeholder type - Source : ICF elaboration on the basis of WCO/IATA/ICAO API Guidelines (2014)

Considering the increase of the number of passengers, Border Control Authorities are faced with a significantly increased workload in identifying and clearing passengers, often with limited resources. At the same time, the professionalisation and internationalisation of organised crime and new and heightened security risks[81], including the threat of terrorism, are developments which necessitate new and innovative measures using new information technologies, such as API systems. The deployment of information technology can be harnessed to ensure that details of arriving passengers are received in advance of the arrival of the flight and thus, allowing the Border Control Agencies adequate time to utilise their resources more efficiently. The table above summarises the rationale for collecting API data by stakeholder type.

[81] For example: Europol (2017), Serious and Organised Crime Threat Assessment (SOCTA), available at: https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment; *Ex-post evaluation of the "Prevention and fight against crime" 2007-2013 Programme (ISEC)*, available at: https://publications.europa.eu/en/publication-detail/-/publication/ba63ddc9-63b4-11e8-ab9c-01aa75ed71a1/language-en

Extent to which the objectives, scope, and definitions set out in the Directive are still deemed to be suitable and fit for purpose

As demonstrated above, there is a strong rationale for collecting API data. However, the evaluation study highlighted a number of issues related to the API Directive as a legal instrument.

Regarding the Directive's objectives, it should be noted that only two objectives out of the four identified in the intervention logic are explicitly mentioned in Article 1 of the Directive (i.e. border control and combating illegal immigration). Although the Directive was adopted as a response to a terrorist attack[82], the legislator defined its objectives in terms of improving border controls and combating irregular migration, limiting themselves to mentioning the added value of passenger data in combating terrorism in a recital and leaving the whole law enforcement component to the national legislator in Article 6(1).

In terms of its scope, definitions and provisions, the main issues identified include *inter alia*:

- **Use of API for law enforcement purposes:** Unlike the PNR Directive which details the serious offences and crimes for which PNR data can be used, the API Directive does not define "law enforcement" and hence, API data can be used very broadly, i.e. for any law enforcement purpose. This reduces the foreseeability of data processing for the data subjects and leads to diverging practices in different implementing countries.
- **Data elements:** Article 3(2) of API Directive provides a non-exhaustive list of data elements which leaves each implementing country the right to request additional data in line with national legislation. These data elements are inconsistent with the elements in the Machine Readable Zone (MRZ) of the passenger's identity document and with the API data elements specified in Annex I of the PNR Directive as well as in the international standards specified by the WCO/IATA/ICAO. This raises questions on the overall relevance of the data-set, and the diverging practices in different implementing countries lead to a burden for air carriers.
- **Types of flights:** The API Directive does not specify whether API data should be collected on all types of flights, as a result of which, flight coverage varies among implementing countries. Implementing countries requesting API data from selected flights do so on the basis of risk analysis and/or policy priorities. The risk-based approach may help saving technical and human resources related to API data collection for both carriers and border control authorities. However, the risk-based approach could result in security gaps as API data is not collected for certain routes considered low risk.
- **Type of carriers:** The API Directive does not specify or define the types of air carriers for which API should be collected; as a result in the majority of implementing countries, API is not collected for charter and non-scheduled flights; however, while the majority of proprietary systems developed by international airlines providing scheduled service rely upon the use of UN/EDIFACT PAXLST messaging transmitted via existing airline communication networks to comply with API data

[82] The Directive was proposed by Spain in 2003 and was adopted in 2004 in response to the Madrid terrorist train bombings.

provision requirements, other entities, such as Charter Carriers, Air Taxi operators, and Executive Air Carriers operate using a differing business model and may not have the technical infrastructure in place to transmit API data with the PAXLST format (WCO/IATA/ICAO Guidelines). This could also be the case for other modes of transport.

- **Geographical scope:** The "API Directive" defines external borders as "the external borders of the Member States with third countries" (Article 2.b). This provision has led to different interpretations of the Directive's geographical scope of application:
  - 1) The Directive's obligations apply to flights coming from outside the European Union (according to this interpretation, carriers operating flights which depart from a Schengen Associate Country are required to supply information on passengers when they are flying into an EU Member State).
  - 2) The Directive's obligations apply to flights coming from outside the Schengen area, irrespective of whether the country of origin belongs to the EU or not.
  - 3) The Directive's obligations apply to flights coming from outside the Schengen area, only if the country of origin does not belong to the EU.

  In addition, some implementing countries and air carriers did raise the question as to the extent to which the Directive would apply in the event of reintroduction of internal border controls by one or several members of the Schengen zone.

5.2. EFFECTIVENESS

The main question addressed in this paragraph is how successful the EU intervention has been in achieving or progressing towards its objectives and corresponding intended impact.

2012 baseline situation on effectiveness

- National authorities considered that API systems contributed to the achievement of the objectives they were set up to address:
- The reduction of irregular migration by improving risk-based profiling of international passengers and increasing the rate of detection of persons identified as irregular migrants;
- The improvement of border control practices primarily in helping border management authorities to better prepare for the control of specific passengers through advance screening of their API data.
- Better preparedness of law enforcement at the EU external border by helping to identify persons posing security risks and other persons including victims of human trafficking and smugglers.

2019 Key findings on effectiveness

- The findings from 2012 are largely confirmed.
- The implementation of the API Directive by implementing countries has contributed to its objectives: (i) improving border control; (ii) combating irregular migration
- It also contributed to the 'specific objectives' identified in the intervention logic: (iii) law enforcement, including in particular (iv) fight against terrorism. The lack of harmonisation in the implementation of the Directive is an obstacle to effectiveness. For example, from the airlines' point of view, the most significant challenge is the lack of standards in the set-up of API systems and the transmission of API data.

Impact on improving border controls

The implementation of API systems has overall been effective for border control purposes and has been positively assessed by stakeholders. By obtaining passenger data in advance of arrival (as soon as the passengers have boarded the aircraft at the airport of departure), border management authorities have additional time to allocate resources and examine possible issues with passengers or their documents and identify those who may require secondary checks upon arrival. However, the extent to which such results have materialised differ significantly across implementing countries and is difficult to quantify in terms of reduced border crossing time as the resources are essentially adapted (to the extent possible) for the known number of problematic cases. In addition, the average processing time for passengers is influenced by other external factors: the introduction of systematic verification and authentication of the travel-document, the systematic border checks in SIS, Interpol's Stolen and Lost Travel Documents (SLTD), and national systems (Regulation 2017/458[83]), and the overall increase in the volume of air passengers.

Impact on combating irregular migration in Member States/EU

The API systems have supported implementing countries authorities in tackling irregular migration. As passenger flows have increased over the years, API systems have been required to process increasing amounts of data used for identifying potential irregular migrants. API systems improved the implementing countries' capabilities to tackle irregular migration, by providing additional time for analysis of information and optimising second-line response by border guards.

Impact on law enforcement, including fight against terrorism

The use of API data is perceived as necessary for internal security and to counter the threat from terrorism. According to stakeholders, the risks of such threats to the European Union remain high, and the added value of API data could be of paramount importance. API systems have had a clear impact on the improvement of internal security, especially when used in conjunction with PNR data.

Based on the stakeholders' replies, it is confirmed that overall the Directive has achieved its objectives.

Factors contributing to or impeding the intended objectives of the Directive

Since 2012, Member States have seen an increased value in using API data for border controls and law enforcement purposes. The factors that stimulated the increased use and appreciation of API data include:

1) Increased volume of air-travel: the increase in the number of air passenger further increased the need for the use API for the border guards to handle efficiently the increased volumes. This need became particularly paramount in the context of the introduction of Regulation 2017/458[84] (the so called "Systematic Checks Regulation), where the use of API is specifically mentioned.
2) Migratory crisis: external threats from irregular migration during the 2013-2017 migration crisis brought in a renewed appreciation and need for the use of API data.
3) Terrorism: the spade of terrorist attacks across the EU has also contributed to increase the recognition of the use of API data.

[83] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0458
[84] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0458

4) International impetus: in recent years the UN has repeatedly called on States to require airlines operating in their territories to transfer API to national authorities to detect departures or attempted entry or transit of suspects with the aim to counter terrorism. In addition, since February 2018, the establishment of national API systems is an ICAO standard, making it mandatory for all Contracting States to the Chicago Convention. Finally, the OSCE Ministerial Council adopted on 8 December 2016, a Decision on enhancing the use of API, whereby OSCE participating States commit, inter alia, to establish a national API system.
5) Increased use of the Schengen Information System (SIS): The quality and volume of data in SIS has increased exponentially. The number of alerts in SIS has grown from 50 million in 2013 to 82 million in 2018[85], transforming the system into a valuable instrument for EU security and border management.
6) Introduction of the PNR Directive: When implementing the PNR Directive, EU Member States have included API data into PNR sets whenever available, as foreseen in the PNR Directive. API data has proved to be a necessary element to enhance the reliability of PNR data significantly.

According to stakeholders, a number of issues have and continue to limit the effective use of API:

1) **Data Quality**: API data is most useful if it is "verified". Incorrect or incomplete data, e.g. due to manual entry related errors, can lead to a waste of resources. With self-check-in (on-line, airport kiosks) process, these issues have been exacerbated.
2) **The time limitation** of 24 hours – Some Stakeholders claim that this limits some of the possible analysis that could be done for border control purpose. Not all PIU/API units operate on a 24/7 basis. Therefore, data arriving on a weekend night may not be processed until the next day. In some Member States, the **use of API data only on selected routes** may have a 'displacement' effect – therefore making criminals change behaviour or use low-risk flights.[86]
3) The limited collection of **API data for in-bound extra-Schengen flights** limits the potential effects of the use of API data.
4) The **separate analysis of API and PNR** is also a limitation that diminishes considerably the effective use of API – the joint analysis could also contribute to border control efforts in addition to law-enforcement.
5) The **API dataset** imposes certain limitations to the analytical value of the data. For instance, seating information and data with regard to luggage, which most carriers already collect, could add value to the analysis in combatting illegal migration and or customs control.
6) The differences between implementing countries in the **use of API data for law enforcement** including **counter terrorism** also shows that there is still room for further development to enhance the effectiveness of the API Directive.
7) The differences observed in each implementing countries' **organisational structures** and API governance create a challenge for carriers, that have to deal with a number of different interlocutors in different countries.
8) The absence of **API data of the crew** has been highlighted by some stakeholders as a possible factor limiting the effectiveness of the measure.

---

[85] EU Lisa Statistical Factsheet 2013 and 2018, available at: https://www.eulisa.europa.eu/Publications/Reports/20140709_factsheet_sis_ii_stats_en.pdf and https://www.eulisa.europa.eu/Publications/Reports/SIS%202018%20statistics%20-%20factsheet.pdf

[86] Interview Member State, Border Guard API Unit.

9) The implementing countries have diverging approaches on **which systems or databases to query**. While the SIS and national watch-lists are often cited, this is not a uniform and systematic practice.

Impact of the Directive on the stakeholders

As highlighted by the evaluation study on the basis of surveys and interviews with stakeholders, the implementation of API systems has affected three key stakeholder groups: competent national authorities, carriers and passengers. The API Directive had a more pronounced impact on the work and resources of national authorities and airlines, with more limited impact on passengers.

Impact on carriers

As regards carriers and their industries, the majority of industry respondents report additional costs related to the implementation of their API systems. Additional challenges stem from the need to ensure the correctness of personal data. Different technological solutions and organisational set-ups across implementing countries further complicated the compliance or lead to increased costs for carriers, even if not all implementing countries chose to sanction carriers. In comparison to the baseline, there is no significant difference in terms of observed or perceived impacts.

Impact on passengers

Overall, the impact the API Directive had on passengers was mixed: a reduction of waiting time for passengers was observed, but not all stakeholders have perceived it as such, as demonstrated by the high number of blank replies (46%) in the corresponding question. It should be noted that the waiting time at border gates for passengers is not only affected by the use of API: for example, while the use of API had a positive impact on processing time during systematic checks, the average processing time for passengers since 2017 has increased due to external factors: the introduction of systematic verification and authentication of the travel-document, the systematic border checks in SIS, Interpol's Stolen and Lost Travel Documents (SLTD), and national systems (Regulation 2017/458[87]), and the overall increase in the volume of air passengers.

Another impact on passengers concerns data privacy and the collection of personal data; however the European Passenger Federation indicated that it has not received complaints in relation to API data collection and processing. Their main explanation of this fact was that most likely passengers were not aware of their data being used for this purpose[88]. This might also be due to the fact that API data is not perceived by passengers as sensitive information, as it concerns data included in travel documents and boarding passes, which are in any case shown to border authorities at the border checks.

Impact on national authorities

There have been several impacts of the Directive on the activities of competent national authorities. One of these relates to the costs incurred due to the set-up and running of targeting centres or the collecting and processing of API data. These costs are discussed in more detail in Section 5.3 (Efficiency) below. The main positive impact has been the increased analytical and investigative capacity of law-enforcement and border

[87] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0458
[88] Interview, 25.06.2019.

authorities, which has translated in increased number of suspected persons identified / and apprehended. Another positive impact is the increased capacity of border guards to clear passengers at the EU external borders, which leads to the facilitation of border control, increased security and better cooperation with other Member States.

5.3. EFFICIENCY

The main question addressed in this paragraph is the extent to which the API Directive has achieved its objectives at a proportionate cost. The analysis comprises:

a) an assessment of the nature and scale of *costs* (including both capital and operating expenditures) associated with the implementation of the API Directive;

b) an assessment of the nature and scale of *benefits*; and

c) a comparative assessment of costs and overall outcomes / impacts.

The analysis does not include the assessment of the necessity and proportionality of the measure as such.

2012 baseline situation on efficiency

Costs of the API Directive

- In 2012, the implementation of API systems entailed varying levels of costs for implementing countries authorities. These differences were partly explained by the cost items included in the calculation of total costs but also the type of API systems developed and the extent to which the systems were implemented. Irrespective of these differences, most implementing countries authorities indicated that API systems have *not* had a significant impact on their operating budgets, which were judged to have been negligible.
- The related compliance costs for carriers, on the other hand, ranged from less than EUR 0.5 million to over EUR 2 million on average per carrier per annum. These costs were seen as substantial by the airline industry. The perception among air carriers was that API systems diverted internal resources from day-to-day commercial activities. In addition to system-related costs, carriers had incurred non-compliance costs in the form of sanctions.

Benefits of the API Directive

- Key benefits of the Directive as reported by national authorities were:
  - *Enhanced border controls*: border control authorities viewed the impact of the collection and use of API data positively, for instance it enabled a faster reaction time against suspect irregular migrants and criminals. Border procedures were also reported to have been improved in the case of certain implementing countries, while second line checks procedures were found to be clearer.
  - *Increased ability to combat illegal migration*: API systems had contributed to curbing irregular migration by targeting suspect irregular migrants better. API systems were also perceived as having brought about an improved knowledge of migration routes and, to some extent, had contributed to an increase in the number of refusals of entry.
  - *A greater number of arrests or increased detention*: some implementing countries reported instances whereby API data checks allowed border control and/or law

enforcement authorities to act against international passengers (presenting a threat to border security), such as deportation and / or arrest. Moreover, API data has been used in combination with other information and evidence for the prevention, detection and investigation of crimes.

- Carriers, specifically air carriers, did not consider that the implementation of API systems brought about direct business benefits. Having to comply with the API Directive requirements implied that resources were diverted away from commercial activities.

Overall cost efficiencies

- The overall efficiency with respect to outcomes associated with API data collection was difficult to measure due to the lack of systematic data that could be used for the assessment. However, national authorities consulted believed that API systems have had an impact at a reasonable cost. None of the authorities thought that API was *not* cost efficient at all, but the perceptions of overall efficiency ranged from very low to very high.
- From the perspective of carriers, the Directive was *not* considered cost efficient as it was *not* perceived as having improved timeliness of flights or general carrier security. Many carriers also felt that having to implement API systems diverted them away from undertaking core business activities, bringing about costly changes to customer practices.

2019 Key findings on efficiency

Costs of the API Directive

- Additional costs derived from the implementation of API systems primarily include: direct costs for implementing countries authorities in terms of setting up and running API systems, compliance costs for carriers, and non-compliance costs (in the event of breaches).
- The overall costs involved in the implementation of API systems varied substantially across the different implementing countries. This can be attributed to different needs and preferences exhibited by Member States, which in turn contributed to differing approaches to implementation and, hence costs.
- Carriers (specifically air carriers), considered that the overall costs entailed by the implementation of API systems were significant and would *not* have been incurred had their implementation *not* been mandated. API-related set-up costs, comprising the acquisition of an appropriate API (data capture) system or the adaptation of the existing IT infrastructure, averaged to less than EUR 0.5 million among air carriers. Recurring expenses were also generally estimated at less than EUR 0.5 million a year. The main cost items reported were API data transmission costs, and general system maintenance costs.

Failure(s) to comply with API Directive requirements have resulted in sanctions for some air carriers, representing lost revenue or investment (had the money been channelled towards other business operations).

Benefits of the Directive

- National authorities recognised that the implementation of API systems has helped drive positive operational outcomes, notably in the area of border control and management.
  - As such, used in conjunction with other border surveillance tools, API systems were perceived to having helped improve the (early) detection of 'high-risk' individuals, thereby increasing national authorities' ability and readiness to identify these individuals, and allowing for better management and deployment of resources on arrival.
  - By furthering a more efficient, risk-based approach to enforcement, it was also considered that API systems may have brought about positive, knock-on effects, notably a reduction in the time taken for border checks and, hence, clearance / 'wait' times for low-risk passengers. However, the evidence pertaining to actual waiting times was mixed.
- It was further recognised that API systems have had a positive influence on national efforts to fight irregular migration and to improve law enforcement and internal security. It was recognised that API systems remained a necessary tool ensuring effective security checks at the borders preventing the entry of people who could have posed the threat (including due to suspicion of involvement in terrorism).

Overall cost efficiencies

- National authorities perceived that the overall costs incurred from the implementation of API systems have been proportionate and are justified, considering the extent of resources used and the nature and level of benefits / impacts achieved to date.
- Carriers, notably air carriers, considered that the costs incurred from the implementation of API systems are only partially or not at all justified, given that (direct) benefits have been minimal for them. In addition, some air carriers were critical of the extent of variation in API-related requirements across implementing countries, which they felt created uncertainties, leading to an increased propensity for non-compliance and, consequently, a greater likelihood of enforcement actions being taken against them.

The main limitations encountered when assessing the efficiency of the Directive in quantitative terms concern the absence of quantifiable data allowing measuring the benefits deriving from the Directive as well as the substantial differences in costs observed in implementing countries.

Overall the research shows that, while national authorities consider the costs incurred to be proportionate to the benefits, air carriers do not share the same view, which confirms the outcome of the previous evaluation exercise. As to whether the same results could have been achieved at a lower cost, stakeholders indicated a number of measures that might have reduced their costs in implementing the Directive. These are:

- Use of standardised requirements to increase coherence across implementing countries as well as data quality, and facilitate data collection/transmission thus avoiding sanctions.

- Use of technical solutions, such as a centralised routing mechanisms, reducing the number of messages that carriers have to transmit.

Below a more detail description of costs and benefits related to the API Directive.

Overview of costs associated with the implementation of API Directive

The API Directive brought about important costs, especially for public authorities and carriers[89]. A typology of the costs incurred by each affected group is set out below.

Direct costs

For carriers specifically, direct costs resulted primarily from compliance activities. One-off, set-up costs have stemmed from capital investments into the acquisition of an appropriate API (data capture) system or the update / adaptation of the existing IT infrastructure. Most carriers outsourced the set-up to a third-party, hence incurring additional costs (e.g. consultancy fees). Furthermore, (some) air carriers explained that the overall process of collecting and transmitting API data to public authorities is managed by a third-party technological solutions provider, in which case initial set-up costs were reported to have been minimal. However, most likely, the provision of API-related services by service providers would have entailed an increase in licence / service fees. These payments are likely to occur on a recurring basis. Other ongoing, operating expenses for carriers include staff costs.

Ad hoc non-compliance costs

Contravening national (API) laws can result in sanctions for carriers. Where such remedial actions have been carried out, they were perceived by some (air) carriers to have been important, notably in terms of their magnitude. Remedial enforcement actions, such as financial sanctions, can be contested in court. Appeals may however present additional (and potentially important) costs for appellants.

Enforcement costs

Public authorities (e.g. border control authorities) faced one-off set-up costs, notably as a result of the acquisition or development of their respective API system (and associated IT infrastructure). Ongoing operating expenses mainly comprise system maintenance costs, staff costs, and other running costs. In some cases, public authorities incurred judicial costs (e.g. adjudication, dispute resolution, or litigation costs), for the review of an enforcement action or as part of appeals initiated by industry.

Indirect costs

Legislation, such as the API Directive, may present 'implicit economic' costs or 'opportunity' costs for regulated parties. These represent the monetary value of what regulated parties forego for channelling resources away from their day-to-day operations to compliance activities. Any cost incurred as a result of complying with the API Directive thus represents an opportunity cost to carriers. As attested by air carriers, compliance costs would *not* have been incurred had the Directive *not* been implemented.

[89] The evidence that is discussed subsequently draws on desk research and consultations held with different stakeholder groups, notably national authorities, carriers, industry representatives and technology service providers in the framework of the Evaluation Study. More detailed information is provided in the accompanying annexes to the main report.

The financial and human resources spent on compliance could have been used for other business activities.

Specific costs for national authorities

Implementation costs of API systems vary substantially across the different national authorities. Implementing countries also have allocated different level of (financial and human) resources to the implementation of API systems. Factors influencing the costs to national authorities include[90]: (1) the (selected) type of API system / technological solution; (2) the type of flights or the number of routes (e.g. inbound/outbound/both; extra-EU/intra-EU/both; etc.) for which API data is collected; (3) the type of checks, assessments and analyses that are undertaken on API data; and (4) the extent to which the implementing countries' respective API systems are integrated with other existing border management systems.

One-off costs

As indicated previously, set-up costs (or one-off development costs) were found to vary across implementing countries. In some implementing countries, notably Germany, Switzerland and Lithuania, the average set-up costs were in the order of approximately EUR 2 million. Similarly, Greece, though having not yet implemented an API system, has an allocated budget of almost EUR 1 million to do so over the next five years[91]. In contrast, at the lower end of the spectrum, estimated costs ranged from as low as EUR 50,000 in Finland to an average of about EUR 200,000 in the Czech Republic and Sweden respectively.[92] Finally, the costs reported by the Italian and Dutch authorities were of a much greater magnitude (when compared to other Member States), averaging to about EUR 9 million.[93]

System specificities and/or implementation particularities may help explain the extent of variation observed in costs reported by implementing countries. Those with higher cost levels, such as Germany, have reported investing in customised API solutions that have seemingly required extensive resources, both internally and externally. Other implementing countries, such as Switzerland, have opted for API solutions that can support more complex (automated) data verification or (data) quality assurance operations. Furthermore, some implementing countries, such as Lithuania, have "single-window" systems in place. These typically support API and PNR transmissions and may have been more costly to develop (owing to their complexity).

---

90 Sources: national research (Evaluation Study); ICF/European Commission. 2012-13. '*Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82*'.

91 The five-year implementation window comprises one year for developing an API system and four years for refinements and maintenance. The estimated costs comprise one-off development costs as well as recurring maintenance costs.

92 Source: interview with Czech border authority / police; Source: quantitative data obtained as part of national research in Sweden.

93 Source: 2012 API evaluation and interview with Dutch API Centre.

Table 2 - Overview of costs for national authorities, in EUR' 000s

MS	Features of API system	Cost item	Frequency	Set-up cost	2012	2013	2014	2015	2016	2017	2018	2019 Jan-May
CH	• Introduced in 2011; fully implemented and operational since 2015	• Initial investments	• One-off	**2,700**[94]	NA	NA	NA	NA	NA	NA	NA	NA
	• API system developed in-house; maintenance undertaken in-house	• Operating / running costs	• Recurring	n/a	**360**	**368**	**237**	**251**	**280**	**341**	**294**	**132**
	• API data is collected at 3 BCPs	• Ongoing development costs	• Recurring	n/a	**163**	**82**	**143**	**160**	**109**	**123**	**59**	**3**
CZ	• First introduced in 2008; fully implemented in 2012	• Acquisition of API infrastructure / IT system	• One-off	**200**	NA	NA	NA	NA	NA	NA	NA	NA
	• The development of the API system was outsourced to an external supplier; maintenance is undertaken by external personnel / third party	• Operating / running costs	• Recurring	NA	NA	**40**	**40**	**40**	**40**	**40**	**40**	**40**
	• API data is collected at five air BCPs											
DE	• Introduced in April 2008; fully operational since then	• Set-up/development costs	• One-off	**1,000**	NA	NA	NA	NA	NA	NA	NA	NA
	• In-house development; Maintenance by an external provider	• Operational costs	• Recurring		**150**	**250**	**100**	**150**	**150**	**210**	**150**	**65**
	• As of 2019, API data is being collected at close to 80 air BCPs											
DK	• Fully operational in 2017; currently being integrated with PNR.	• Set-up[95] costs	• One-off	NA	NA	NA	NA	NA	NA	**310**	**360**	NA
	• API data is collected at 10 air BCP to air carriers on all flights	• Operational costs	• Recurring	NA	NA	NA	NA	NA	NA	NA	NA	**150**
EL	• API system not developed yet		• One-off	NA	NA	NA	NA	NA	NA	NA	NA	**900**[96]

[94] Capital expenditures incurred over the period 2007-11.

[95] The one-off set-up costs relate to the initial API system developed by the Danish authorities. Additional costs are foreseen during the integration of API and PNR systems. These are expected to amount to almost EUR 7 million. Operational costs are also expected to increase, amounting to about EUR 1.3 million on a yearly basis. These will include maintenance costs as well as licence fees.

MS	Features of API system	Cost item	Frequency	Set-up cost	2012	2013	2014	2015	2016	2017	2018	2019 Jan-May
LT	• First introduced in 2016; a single-window model (gathering both API and PNR data) implemented in 2017 • API data is collected at four air BCPs • API system developed in-house; maintenance is also in-house	• Initial investments	• One-off	NA	NA	NA	NA	NA	NA	**1,785**[97]	NA	NA
NL	• First introduced in 2009; fully implemented in 2017 • API data collection mandated to air carriers on inbound extra-EU/Schengen flights • API system developed partly in-house and via a third-party; maintenance both in-house and external personnel • API data is collected at six air BCPs	• Initial investments	• One-off	NA	NA	NA	NA	NA	NA	**10,000**[98]	NA	NA
SE	• Fully implemented in 2018 • API data collection mandated to air carriers on inbound extra-EU/Schengen flights • API system developed in-house; technological solution purchased from a third-party	• Staff costs (involved in API system set-up) • Staff costs	• One-off • Recurring	NA NA	NA NA	NA NA	NA NA	NA NA	NA NA	**343**[99] NA	NA **170**	NA **170**

Source: ICF – Evaluation Study. Notes: (1) 2011 is the baseline year; (2) 2019 figures are provided for the months January to May; (3) all figures have been rounded to the nearest thousand; (4) figures provided in local currencies have been converted into euros (at the market rate prevailing at the time of writing); (5) 'NA' denotes 'not applicable;' (6) 'n/a' denotes 'not available'

[96] Current estimate provided by Greek authorities for upcoming implementation of API system, expected to be over the coming 10 months.
[97] Costs pertain to development costs associated with a data capture system for both API and PNR.
[98] Capital investments expected to have been made over the implementation period, i.e. from 2009 (when API system was first introduced) to 2017 (when API system became fully operational).
[99] The relevant Swedish authority explained that there were no capital costs involved during the initial set-up; only staff costs as the system was developed in-house (with 6-8 employees, each paid between SEK 40,000 (EUR 3, 800 and SEK 45,000 (EUR 4,000)). A mid-value has been calculated by computing an average of the low-end (6*EUR3,800*12) and high-end (8*EUR4,000*12) values which is about EUR 343,000 (rounded to the nearest thousand). The exact period of time during which these costs were incurred is not known. They are however likely to have been incurred prior to 2018 as an API system was fully in place in Sweden by 2018. Assuming that it takes at least one year to develop the system, we believe that these one-off costs took place in 2017 Source: interview with API / Targeting Centre.

Recurring costs

Operating expenses also appear to vary substantially across implementing countries. As it can be reasonably expected, Member States that accommodate larger passenger flows tend to incur higher year-on-year running costs[100]. Germany, for instance, faces on average EUR 200,000 every year in running / maintenance costs. In other smaller implementing countries, however, recurring expenses were almost on par with those observed in larger implementing countries. As such, on average, Denmark, Sweden and Switzerland face about EUR 250,000 costs every year[101]. This could however be explained by certain contextual factors, notably higher labour costs in these countries. Currently, Switzerland has the highest (estimated) hourly labour costs (in Europe) at almost EUR 55.0 per hour, followed by Denmark and Sweden at almost EUR 45.0 and EUR 40.0 per hour respectively.[102] Staff costs, typically accounting for a large part of recurring costs, could thus explain the significance of overall operating costs observed in these implementing countries.

Specific costs for carriers

One-off costs

Carriers generally considered the implementation costs of API systems as significant. They further recognised that such costs would *not* have been incurred had their implementation *not* been mandated. API-related set-up costs were estimated at less than EUR 0.5 million.[103] As stated previously, initial set-up costs primarily resulted from the adaptation of air carriers' existing IT systems / infrastructure to ensure that they were are in line with the requirements of the API Directive.

Among a few larger carriers, however, initial set-up costs were contained and less burdensome[104]. These carriers explained that the API Directive did not entail direct costs for them per se since third parties, notably technology service providers (e.g. Amadeus, SITA, etc.), were liable for undertaking the necessary changes and adapting their existing product offering to incorporate the capture of API data. Some costs were nonetheless borne by the air carriers in question, though these were generally perceived to have been minimal.

Recurring costs

API-related operating costs were generally estimated at less than EUR 0.5 million a year.[105] For one mid-sized air carrier, for instance, annual operating costs range from EUR 9,100 to EUR 13,600 and relate primarily to fees paid to an external service

[100] For instance, there may be a need to recruit more staff or to carry out more frequent systems maintenance to deal with larger batches of API transmissions.

[101] In Sweden, monthly salaries are reported to range between EUR 3,300 and EUR 3,800, suggesting that recurring staff costs for the authority concerned average to about EUR 170,000 every year.

[102] Source: Eurostat (2018).

[103] Please note that there is no clear-cut evidence on the magnitude of costs incurred by different types of carriers from the implementation of API systems. As such, for most carriers, it would appear that these costs are difficult to estimate. Some estimates have nonetheless been gathered from air carriers specifically. While these findings shed some light on costs, they ought not to be generalised for other stakeholder groups (i.e. other transport operators), owing to (potential) differences in their approach to implementation (e.g. varying system specificities, etc.).

[104] Source: interviews with three mid-to-large -sized air carriers. Size is based on revenue, number of routes / countries / destinations served, and the number of passengers carried.

[105] Source: survey conducted with carriers and industry representatives (as part of the Evaluation Study).

provider for the transmission of API data to authorities on their behalf.[106] A cost breakdown by carrier size is less clear, though one could expect costs to be proportional to the number of API transmissions. Larger carriers, i.e. those serving multiple routes and/or offering an extensive array of flights, are therefore likely to be facing higher transmission costs and overall recurring costs respectively.

In addition to the above, air carriers argue that the existing set up creates a competitive disadvantage for air transport as compared to other modes of transport, due to the burden for air passengers and industry associated costs (compared to maritime, train and coaches/buses operators).

Other costs

Some of the larger carriers consulted expressed concerns about *ad hoc* costs, specifically those driven by sanctions.[107] These air carriers were mainly critical of the lack of a consistent approach among different implementing countries in defining and interpreting breaches (or, in other words, clearly communicating expectations for the minimum acceptable level of (API) data quality). Differing approaches in enforcement were thus perceived to be hampering compliance efforts and increasing the risk of non-adherence and potential corrective actions being imposed by national authorities. It was believed that the overall cost to / impact on carriers (of the differences observed in enforcement regimes across Europe) to be the revenue lost (where financial sanctions were imposed) as well as the burden associated with having to abide by different rules across the implementing countries. An estimate of the latter was not gathered during this research. There is nonetheless evidence pertaining to the (monetary) size of financial sanctions, which has been in the order of EUR 4,000 on average, per breach (i.e. where API transmissions were incomplete or not received by national authorities), in some Member States (including Austria, the Netherlands, and Poland). Sanctions have generally been higher in Germany, where they reached an average of EUR 6,000 per breach. By law, German authorities are able to impose sanctions of up to EUR 50,000, much higher than other Member States (where the permitted maximum averages to about EUR 5,000), which could help explain the higher sanction levels generally observed.

Benefits of implementing API systems

Operational benefits

The implementation of API systems helped drive positive operational outcomes, notably in the area of border control and management.[108] API systems constitute an effective border management tool for national authorities and it is recognised that they have contributed to improved border control activities, notably by increasing the relevant authorities' preparedness and readiness, in terms of identifying high-risk individuals ahead of their arrival and by expediting the process of passenger checks upon arrival.

With API systems in place, national authorities are able to screen passenger lists and detect any suspicious individuals ahead of flight arrivals. The API data received is used to query various systems, in particular SIS, allowing for a 'fuzzy[109]' or 'approximate'

[106] Source: interviews with air carriers (as part of the Evaluation Study).
[107] Source: interviews with two mid-to-large -sized carriers.
[108] Source: interviews with national authorities, notably BG, CZ, EE, EL, NL. SI, SE.
[109] https://en.wikipedia.org/wiki/Approximate_string_matching

search. Such a 'fuzzy' search will require more time and may result in false-positives that need to be evaluated. The very short physical border-control process does therefore not allow such 'fuzzy' searches. Evidence pertaining to the proportion of 'suspicious individuals' identified through API data checks at implementing countries' external borders is limited and the number of hits vary substantially across countries, owing to various contextual differences, such as the type of national databases used, the decisions on what type of data against which API data are matched, etc. Nevertheless, a shared perception among consulted stakeholders is that API data have allowed national authorities to identify and analyse risks posed by certain passengers more efficiently.

By furthering a more efficient, risk-based approach to enforcement, it was also considered that API systems may have brought about positive, knock-on effects, notably a reduction in the time taken for border checks and, hence, clearance / 'wait' times for low-risk passengers.

Wider policy and societal benefits

API systems are considered to have had a positive influence on national efforts to fight irregular migration and other associated criminal activities and to enhance law enforcement and internal security. However, the full scale of benefits realised on the ground is difficult to estimate. This is because API systems constitute one of the numerous tools used in combination by national authorities in the areas of migration control and law enforcement.

The API Directive is considered to helping combat irregular migration, notably by increasing the capacity of border control authorities to identify fraudulent documents and the capacity of law enforcement authorities to identify high-risk passengers and detect and prevent migration crime. The Croatian and Latvian authorities estimate the impacts of the collection of API data on the identification and arrest/detainment of high-risk individuals to having been quite or highly important. Furthermore, the evidence gathered indicates that API data checks can allow implementing countries to increase security at their borders, for example by identifying and refusing entry to passengers judged suspicious or 'high-risk.' In Finland (see Figure 6 overleaf), for instance, of the 10,400 passengers who were refused entry over the period 2014-19, about 150 passengers (or almost 2 per cent) were identified through API data checks.

The implementation of the API Directive was further considered to be necessary for implementing countries' actions targeted at increasing/preserving internal security and public order. Implementing countries report they use, and consider API necessary for fighting terrorism. As such, the ability to match API data against national/EU/foreign counter-terrorism and counter-organised crime databases was recognised to providing relevant authorities with necessary information and better targeting security checks at the borders

The quantification of such benefits is however difficult to undertake. API systems are widely and commonly used in conjunction with other border surveillance and law enforcement tools, making it difficult to isolate their impacts on wider societal outcomes, such as internal security.

Member State	CH	CZ	FI	HR	IE	LT	MT	NL
Period covered	2016-19	2012-19	2014-19	2017-19	2018-19	2016-19	2016-19	2017-19
Mode(s) of transport for which API data was gathered	Air	Air	Air, sea, land	Air	Air	Air	Air	Air
# hits (national databases/police watch lists/other)	tbc	tbc	3,000	10,100	600	9,000	tbc	36,000
# hits (other EU databases)	32,025	7,000	1,000	200	n/a	3,000	n/a	n/a
Total (# hits)	**32,025**	**7,000**	**4,000**	**10,300**	**600**	**12,000**	**tbc**	**36,000**
# overall international passenger arrivals	25,747,000	18,945,000	40,570,000	15,176,000	53,802,000	18,783,000	8,955,000	29,896,000
# passengers for whom API data has been collected	10,774,000	16,716,000	40,570,000	1,003,400	6,825,000	5,507,000	4,847,000	29,896,000
% passengers for whom API data has been collected	42.0%	88.0%	100.0%	7.0%	13.0%	29.0%	53.0%	100.0%
% passengers for whom a hit was detected	**0.3%**	*	*	**1.0%**	*	**0.2%**	**tbc**	**0.1%**
# passengers ultimately identified as 'high-risk' individuals	n/a	n/a	n/a	3,500	n/a	n/a	n/a	n/a
# 'high-risk' individuals identified at the border thanks to API data collected	n/a	n/a	n/a	n/a	n/a	n/a	600	n/a
% individuals identified as 'high-risk' thanks to API data collected	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**
# passengers refused entry at BCPs	5,000	2,200	10,400	n/a	n/a	2,000	n/a	n/a
# passengers refused entry thanks to API data collected	n/a	n/a	150	600	n/a	n/a	n/a	n/a
% individuals refused entry at BCPs thanks to API data collected	**n/a**	**n/a**	**1.5%**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**

Figure 6 Extent of detection of 'high-risk' individuals from API data checks. Source: ICF - Evaluation Study - quantitative data provided by national authorities (as part of national research). Note: (1) figures are rounded to the nearest thousand; (2) 'N/A' denotes 'not applicable; (3) 'n/a' denotes 'not available;' (4) 'tbc' denotes 'to be confirmed;' (5) '' denotes a very small number or percentage; (6) the proportion of passengers for whom a hit was detected is calculated as: [total (#hits) / # passengers for whom API data has been collected]*100; (7) the proportion of individuals identified as 'high-risk' thanks to API data collected is calculated as follows: [# 'high-risk' individuals identified at the border thanks to API data collected /# passengers ultimately identified as 'high-risk' individuals]*

5.4. COHERENCE

The main questions addressed in this paragraph are, on the one hand whether, a) the objectives and purposes of API systems in Member States are consistent with the Directive, b) The Directive is coherent with other relevant EU legislation. On the other hand, we also assess the coherence of the Directive with the international regulatory framework on passenger information (e.g. the Chicago Convention).

2012 baseline situation on coherence

- The objectives outlined in related EU legislation, national legislation, as well as those driving the implementation of API systems, were considered compatible with those of the API Directive.
- However, in practice, the national implementation by some implementing countries was not fully in line with Data Protection legislation. The main data protection issues identified related to the length of time for which API is retained and the purpose for which it was used and the number and position of persons who had access to the data. In addition, some national legislation did not fully and accurately transpose data protection obligations on the storage and deletion of the data.
- The 2012 evaluation also anticipated potential coherence issues arising with the introduction of the then proposal for a PNR Directive. Potential coherence issues mentioned were around similar data elements and the distinction between the main purposes of both Directives.

2019 Key findings on coherence

- The objectives of the national API systems are aligned with the objectives of the API Directive, although as a result of the Directive's minimum requirements, the implementation of API systems shows a fragmented picture.

- There are several discrepancies between the API Directive and the PNR Directive causing operational challenges in practice. The main coherence issue relates to the lack of clarity on the use of API data for law enforcement purposes and the differences in data protection frameworks in the API and PNR Directives, specifically regarding data retention periods.
- The ETIAS/EES/(VIS) Regulations contain requirements for carriers (air, sea, land (but not trains) to query these central systems with personal data captured from the travel document(s) in order to determine if the carrier should let the person board (OK) or not (Not OK). This query contains (nearly) the same data as the data received under the API Directive. The carrier industry calls this query: Interactive API or iAPI.
- A future API instrument could re-use the data sent under the ETIAS/EES(VIS) Regulations for purposes specific to the API instrument and thus prevent passengers, carriers and service providers of needing to provide the (nearly) identical data twice.
- The passenger relies on the query to ETIAS/EES/(VIS) to use accurate and complete personal data to prevent falsely denying boarding. The Member State authorities rely on accurate and complete API data to support the purposes of the API instrument. Capturing those data in a single moment for different purposes as specified in multiple legal instruments could be beneficial.
- The API Directive is not fully coherent with the international regulatory framework on passenger information to the extent that flight and passenger data fields included in the API Directive do not correspond to those currently agreed and prescribed in international instruments and standards.

The national API systems and the API Directive

The objectives and purposes of API systems in the implementing countries are to a certain extent aligned with the objectives of the API Directive. The primary objectives of the API Directive are to improve border control and combat illegal migration, while leaving the option to implementing countries to also use collected API data for law enforcement purposes. The current state of play of the transposition and implementation of the API Directive shows that most implementing countries have set up their API systems to enhance external border controls and fight irregular migration. Additionally, most implementing countries have also made use of the possibility to process API data for law enforcement purposes.

The extent to which API systems are coherent with the provisions of the API Directive must also be analysed considering that many of the provisions of the Directive – ranging from the list of API data elements which can be requested, the transmission modes and messaging protocols to the governance structures involved in the collection and processing of data – are only setting minimum requirements on implementing countries.

When considering API Directive's minimum requirements, national API systems are aligned with the provisions and objectives of the Directive to the extent that nearly all implementing countries (with the exception of Cyprus, Greece, Iceland and Norway which have not yet set up a fully operational system to request API data) collect the API data elements as listed in the Directive and do so on inbound extra-EU/Schengen flights. However, as a result of these minimum requirements, the implementation of API systems reflects a fragmented picture on other important aspects:

1) **Data fields**: The non-exhaustive API data elements listed in the Directive result in implementing countries requesting additional data (e.g. gender, seat and luggage information, and crew data).

2) **Type of flights**: Most implementing countries request API data on all flights[110] and from all carriers[111], while some others request API data only on selected flights[112] and/or only from certain carriers[113] due to technical and human resources constraints.
3) **Technicalities**: The Directive is neither prescriptive on the messaging protocols nor on the modes of transmission, only stating that these should be 'electronic'. This is currently a source of incoherent implementation of the Directive across implementing countries.
4) **Law enforcement purpose**: Lastly, the option left to implementing countries to use API data for law enforcement purposes, without providing a clear definition of this purpose nor laying down a framework for processing data, led to a disjointed implementation at national level. In particular, this affected a coherent approach on the transmission of API data to national authorities responsible for border control and a consistent approach on data retention by national authorities.

The API Directive and other obligations under EU legislation
Since 2012, the EU policy landscape in areas such as border management, law enforcement and data protection has changed significantly. Therefore, in order to assess the API Directive's coherence with relevant EU instruments, the analysis has to tackle separately each of the three dimensions.

Border management and combating irregular migration
Collecting API data at external borders enables national authorities to cross check passenger data against information contained in EU level databases and to do so before the passenger actually shows up at the border crossing point thus enabling more accurate and in-depth checks. Such in-depth check rely on "fuzzy" or "approximate searches" requiring more time to process and more time to eliminate false matches, making them inappropriate for first-line border-control.

In terms of coherence with other instruments adopted under the Schengen *acquis*, currently border checks at the EU external borders are regulated by the Schengen Borders Code.[114] Regulation 2017/458[115] (the so-called "Systematic Checks Regulation") amended the Schengen Borders Code to extend to EU citizens the mandatory checks against relevant databases such as SIS and Interpol's SLTD on the occasion of the crossing of an external border. The Schengen Borders Code provides that border checks may be carried out in advance on the basis of API. This possibility is not fully exploited in practice by implementing countries[116], limiting the complementarity and use of synergies between these two instruments. The research did not find evidence of implementing countries requesting API data on intra-Schengen flights based on the exception of introducing temporary internal border controls in accordance with the Schengen Borders Code (Chapter 2 of Title III).

[110] AT, BG, CZ, EE, ES, HR, HU, IE, IT, LT, LV, MT, NL, PT, SE, SI, UK, RO, FI, IS.
[111] AT, BG, CY*, CZ, DK, EL*, ES, FR, HU, IE, LT, LV, SE, SI, UK, FI, IS, LU, MT.
[112] CH, DK, FR, PL, NO*, DE, LU.
[113] BE, CH, DE, EE, HR, IT, NL, NO, PL, PT, RO, SK.
[114] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0399
[115] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0458
[116] See the ongoing assessment carried out by ICF of the implementation of Regulation 2017/458 as regards the reinforcement of checks against relevant databases at external borders.

While a majority of implementing countries check API data against SIS and Interpol SLTD, this is less systematically done regarding the Visa Information System (VIS).[117] The list of API data elements also does not include the visa-sticker-number which would allow effective comparison against the VIS register.

However, the VIS recast[118] also includes the mandatory verification of a valid visa via an interactive consultation of the VIS by the carrier at check-in.

The Entry Exit System (EES), once fully implemented[119] is an information system interlinked with VIS which aims to enable Member States to identify third-country nationals who stay in the Schengen area, Bulgaria or Romania beyond the authorised time.[120] The EES will apply to all non-EU citizens admitted for a short stay (maximum of 90 days within any 180-day period) in the Schengen area, Bulgaria or Romania. When crossing the border, the system records the contents of the passport's Machine-Readable Zone (MRZ) and chip, biometrics and the date and point of entry and exit, making it possible to detect overstaying and to verify whether third-country nationals holding a short-stay visa for one or two entries have already used the number of entries authorised by their visa.

The European Travel Information and Authorisation System (ETIAS), once fully implemented[121], will enable the advance authorisation of visa-exempt travellers when crossing the external borders and will in particular impose a new check to be carried out by carriers to those travellers. While currently carriers only check whether visa-exempt travellers have a travel document, with ETIAS, carriers will also check whether they have a valid travel authorisation. Travellers will have to make an online application to obtain an ETIAS travel authorisation prior to travelling to the Schengen area. At check in, air and waterborne carriers, as well as carriers transporting groups overland by coach, will have to verify the status of the travel document required for entering the Schengen area, including verifying the validity of the ETIAS travel authorisation. The carrier will send a query to the carrier gateway and will receive an "OK/NOK" response. A carrier can still board a traveller that received a NOK answer at its own risk.

The "carrier gateway" to be set up by eu-LISA for the EES (which consults the VIS) and for ETIAS stems from different provisions but will be based on industry practices and standards that are commonly defined by industry as Interactive API. Indeed, the EES and ETIAS Regulations require carriers to carry out queries for travel authorisations for visa holding third-country nationals and visa exempt third-country nationals, respectively, through the introduction of the interactive query (Article 13 of the EES

---

[117] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008R0767

[118] https://ec.europa.eu/home-affairs/news/eu-visa-policy-commission-upgrades-visa-information-system-better-secure-external-borders_en

[119] At the moment of writing this document, the EES is expected to be fully implemented in the first quarter of 2022. This date is however not legally binding and is subject to the conclusions of close project monitoring.

[120] See Article 11(4) of Regulation 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[121] At the moment of writing this document, the ETIAS system is expected to be fully implemented in the fourth quarter of 2022. This date is however not legally binding and is subject to the conclusions of close project monitoring.

Regulation and Article 45 of ETIAS Regulation). With the emphasis on the use of industry standards[122], the industry-recommended technology for facilitating this[123], is an interactive Advance Passenger Information (iAPI). The standard iAPI messages provide the information required to query EES and ETIAS (i.e. they contain the MRZ data) and the message formats are firmly established as part of the carriers' departure control system (DCS). Hence, a "carrier gateway" is a necessity to enable the interactive query against one-way extracts[124] of the EES and ETIAS databases.

The established carrier processes are unsuited to apply separate procedures for EU Citizens (or persons enjoying free movement in general) and third-country nationals. All carriers will hence query ETIAS/EES/(future VIS) for all passengers where the "carrier gateway" will discard data from EU citizens and reply 'non-applicable' for ETIAS (including VIS)/EES purposes.

The personal data (captured from the Machine Readable Zone) to query ETIAS/EES/(VIS) will be captured, transmitted and processed for ETIAS/EES/(VIS) purposes. This personal data is however (nearly) identical to the data captured, transmitted and processed under the API directive.

In order to prevent passengers and (air) carriers to capture and send personal data once for EES and ETIAS query purposes and in addition capture and send the same personal data for "batch API" (and PNR) purposes to the Member State of destination, the data exchange could be simplified by having the same message sent once to a Centralised Routing Mechanism[125] from where it can be forwarded to different destinations (read-only extract of ETIAS/EES, then various Member States' authorities). This could, in turn, also lead to rationalising batch API and PNR data transfer at national level.[126]

While this development is supported by industry associations, at national level, stakeholders consulted are sceptical. Whilst the latter acknowledged the benefits such integration could bring (faster data processing, increased security, better integration with other relevant systems, more clarity for air carriers and improved passenger experience), several implementing countries also highlighted a number of (expected) challenges to fully implement iAPI such as the lack of financial resources and insufficient analytical and processing capacity.

Law enforcement and security

The API Directive regulates the collection of API data for border control purposes, and allows the collection and transfer of API data for law enforcement purposes on the basis of national law. In addition to this, in 2016, the EU PNR Directive has established an obligation for air carriers to transmit API data, in addition to reservation data, whenever API data is collected in the normal course of their business. In this case the data in question become part of PNR data set. In practice, API data has proved to enhance the

[122] 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.

[123] ICAO WCO IATA Management Summary on Passenger-related Information (Umbrella Document), par. 30.

[124] The term "one way extracts of the EES and ETIAS databases" insists on the fact that carriers do not access operational systems but extracts of the database that only contain the data relevant for the intended queries. Further, that the extracts can only be refreshed by downloads from the operational systems but that data cannot be uploaded towards these systems, to seal them off any intrusion from non-authorised users.

[125] A central point to which air carriers may submit passengers and crew manifests and which can forward the passengers data to other information systems.

[126] Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information and Passenger Name Records.

reliability of PNR data significantly, due to the nature of the API data which is often collected through the MRZ (as opposed to the declarative nature of PNR data).

There are several discrepancies between the API Directive and the PNR Directive, causing operational challenges in practice and leading to a lack of clarity for air carriers and data subjects.

The use of API data for law enforcement purposes is possible under the API Directive, however the Directive lacks a definition of 'law enforcement'. In practice, the national implementation of this purpose ranges from enhancing internal security and public order, to fight against terrorism as well as to ensure national security, arguably going beyond the objectives of Article 6 of API Directive. This suggests a wider understanding of the concept of law enforcement than the one included in the PNR Directive[127], which is expressly limited to the use of data for the "prevention, detection, investigation and prosecution of terrorist offences and serious crime".

In practice, air carriers are obliged to transmit API data under the API Directive and to transmit API data (if collected by air carriers in the normal course of their business) under the PNR Directive. However:

1) The API data elements do not entirely match in the two Directives.[128]
2) The two Directives do not apply to the same type of flights - Air industry and technical providers representatives have stressed the need for clarity in terms of availability of API data as part of PNR as compliance with PNR does not impose availability of API data.
3) The geographical scope of the two directives does not coincide as the API Directive is building upon the Schengen acquis, while the PNR Directive is not as it only applies to EU Member States (with the exception of Denmark, who does not participate in the PNR Directive on the basis of Protocol 22).

These elements impair the consistent collection, processing and use of API data and the existence of these inconsistences is considered by some stakeholders as a gap in both border management controls and law enforcement in the EU.[129]

EU data protection framework

When describing data processing, the current text of the API Directive refers to Directive 95/46 EC[130], the so-called "Data Protection Directive". This Directive applied until 25 May 2018, when it was replaced by EU General Data Protection Regulation (GDPR).[131] Thus, this coherence analysis considers the two data protection instruments while acknowledging that Directive 95/46/EC applied during most of the evaluation period. It should be noted that this analysis is separate from an examination of potential

[127] Source: Desk research and EU level interviews.

[128] The PNR Directive refers to "Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)". Gender is not a mandatory API data element included in the API Directive.

[129] Source: EU level and national interviews.

[130] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereafter the 'Data protection Directive'.

[131] 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) https://eur-lex.europa.eu/eli/reg/2016/679/oj.

inconsistencies between the implementation of API systems by implementing countries and data protection requirements at EU level.

When solely comparing the data protection principles referred to by the API Directive, no inconsistencies appear with those included in Directive 95/46[132]. However, since 2018, the EU General Data Protection Regulation (GDPR) significantly strengthened the EU data protection framework, strengthening the obligations of data controllers and the rights of data subjects.[133] Like Directive 95/46, the GDPR also establishes firmly and explicitly the principle to set a limitation to retain data which is necessary and proportionate to the purpose of the data collection. For example, the list contained in Article 3 of the Directive is a minimum list of data elements and not a closed list. From a data protection perspective, an exhaustive list of data elements (e.g. in an Annex to the Directive) would be needed to ensure consistency with the principle of processing only data which is necessary for the purpose for which they were collected and thus implement a less intrusive approach to the passengers' right to privacy. Overall, any API data element to be collected would need to meet the requirements of necessity and proportionality.

The API Directive establishes the retention of data for border control purposes to 24 hours. Considering the purpose of the data collected and the processing time to perform border checks, the 24-hours-limitation appears to be proportionate. However the possibility for national authorities to retain data for longer than 24 hours, if "needed for statutory functions", as provided for by Article 6, does not include clear data retention requirements. A practice observed in the transposing legislation of a few implementing countries, is to include data retention limitations (which exceeded 24 hours) in such exceptional cases as well.[134]

The main coherence issue emerging from the analysis relates to the use of API data for law enforcement purposes and the differences in data protection frameworks in the API and PNR Directives. The API Directive left the option for implementing countries to also use API data for law enforcement, yet the purpose of using data in this case remains vague and no other limitations regarding data retention are set. An unclear definition of the purpose for which personal data is used impairs clarity and foreseeability for data subjects and hence their right to the protection of personal data. Since the transposition of

[132] The principles mentioned in the API Directive refer to the principle of purpose limitation (recital 12), definitions of 'personal data, 'processing of personal data' and 'personal data filing system' (Article 2(e)), data retention timeframes (Article 6), use of personal data for law enforcement purposes (Article 6), obligation to inform the passengers (Article 6) – which are aligned to those of Directive 95/46.

[133] For example, the definition of personal data was updated in the GDPR, which now includes genetic data (Article 4(1) GDPR). The definitions of 'filing system' and 'processing' [of personal data] included in the GDPR are substantially the same as those included in the data protection Directive. In terms of definitions however, GDPR includes a wider range of concepts, defining 'biometric data' and 'cross-border processing' [of personal data] among others, updating EU data protection framework to current technological and social changes. The GDPR has considerably enhanced the rights to information and access to personal data (Articles 12, 13 and 14) compared to the rights included in the former data protection Directive (Article 10 and 11 of Directive 95/45). This includes for example the need to establish a data protection officer, obligation to set a storage time for which data is retained and inform the data subject about it.

[134] For example, in France, for the purpose of external border control, API data may be consulted for a period of 24 hours from the date of their transmission. By way of exception, this period is extended to 12 days for personal data relating to persons concerned only in the following cases: delayed flights, diverted flights, use of decoupled tickets, presentation at the entrance to the territory after a certain period of time, keeping in the waiting area, refusal of entry, fine procedure for the carrier. For the purpose of fighting against irregular migration, API data can be consulted for up to 6 months after their transmission.

the API Directive, Directive 2016/680[135] applicable to the processing of data by law enforcement authorities establishes that EU Member States and Schengen associated countries should provide "appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage for personal data".

In coherence with other EU legislation relevant in this case, the PNR Directive limits the use of data to a closed set of offences clearly listed in Annex II of the Directive and referring to most of the offences included in the European Arrest Warrant.[136] This approach provides clarity as to the scope of the data processing. The same is not valid for the API Directive, which only refers to a general notion of "law enforcement", leaving further details to national legislation and lacking an analysis of the necessity and proportionality of the use API data.

The API Directive and the international regulatory framework on passenger information

For the purpose of the current evaluation, the coherence of the API Directive with the following international instruments was analysed:

- Annex 9 (Chapter 9) to the Convention on International Civil Aviation (Chicago Convention)[137]
- WCO[138]/IATA[139]/ICAO[140] API Guidelines[141]
- UN Security Council Resolutions 2178(2014), 2309(2016) and 2396(2017),
- OSCE Ministerial Council Decision 6/16 of 9 December 2016 - Enhancing the use of Advance Passenger Information.

The API Directive is not fully coherent with the international regulatory framework on passenger information to the extent that flight and passenger data fields included in the API Directive do not correspond to those currently agreed and prescribed in international instruments and standards. This concerns mainly specific API data fields as well as data transmission and messages protocols.

Compared with the API Directive, guidelines and standards agreed at international level provide a more detailed list of API data elements. Thus, the API data fields mandated in the API Directive fall short of what is recommended practice at the international level. The API Directive was drafted with the spirit of 'minimum harmonisation'. It does not reflect all measures and technicalities that are applied at national level nor standards agreed by the primary stakeholders collecting and transferring API data, namely the aviation community. This point may not be strictly a point of incoherence as the API

[135] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584529834913&uri=CELEX:32016L0680
[136] Art.2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.
[137] See https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf.
[138] World Customs Organization - http://www.wcoomd.org/en.aspx
[139] International Air Transport Association - https://www.iata.org/
[140] International Civil Aviation Organization - https://www.icao.int/Pages/default.aspx
[141] The API Guidelines were initially developed in 1993 by the WCO in cooperation with the International Air Transport Association (IATA). Subsequently, the International Civil Aviation Organization jointed the process and a 'Contact Committee' comprising the three organizations was formed. In order to help their respective members implement the API system, the three organizations have jointly published the WCO/IATA/ICAO Guidelines on Advance Passenger Information in 2003, 2010 and in 2013. Source: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx.

Directive does not collect data which is contradictory to international standards. However, the fact that flight information and passenger data listed in the API Directive is not exhaustive may be conflicting in practice with the more detailed and closed list of data established in IATA/WCO/ICAO Guidelines and Annex 9 to the Convention on International Civil Aviation.

Similarly, there is a mismatch between the rather vague formulations of the API Directive on messaging formats and messaging protocol of API data transmission compared to the standards agreed upon at international level (e.g. UN/EDIFACT PAXLST).[142] The implementing Commission Decisions of the PNR Directive lists these updated data formats and transmission protocols. Thus, in cases where API data is transmitted to national authorities within the scope of PNR Directive, API data transmission is aligned with the international regulatory framework.

Another inconsistency concerns the 'geographical scope' of API data collection. The API Directive sets out provisions for the collection of API data on external in-bound flights to implementing countries.[143] The international regulatory framework does not include such limitation: API data should be collected on all inbound, outbound and transit flights. This was reinforced with calls from the UN to its Member States to collect API data to ensure and improve fight against terrorism and the phenomenon of 'foreign terrorist fighters' and calls to create the necessary conditions for automatic cross-checking of API data with other international and national databases.[144]

5.5. EU ADDED VALUE

This section presents the main benefits of this EU intervention. The main question addressed in this paragraph is what would have happened without the Directive. The possible unintended effects of the Directive are assessed, as well as what measures would have been put in place by implementing countries without action at EU level.

2012 baseline situation on EU Added Value

- The majority of the national competent authorities considered that the Directive brought added value with respect to adoption of the API systems and the increased capacity to process information faster to identify irregular migrants and suspected criminals (e.g. the national authorities in charge of border control and law enforcement adopted API systems, technology and related practices faster).
- The fragmented implementation of the Directive across implementing countries reduced its added value. In some implementing countries there was not a strong business case to support the implementation of API systems.
- Most air carriers questioned the added value of the Directive in its current form. The information was already collected in air carriers' departure systems and it did not allow stopping suspicious persons from boarding the plane, hence not specifically improving carrier's (in-flight) security. It did not specify standards or guidelines which

[142] Available at: http://www.unece.org/trade/untdid/d05b/trmd/paxlst_c.htm
[143] Please see under "relevance" regarding interpretative issues on the geographical scope of the API Directive.
[144] https://undocs.org/S/RES/2396(2017)

would have enabled more joined up implementation.

- Unintended benefits were the adoption of border control practices, the widespread investment in and the adoption of enhanced border control technologies.

2019 Key findings on EU added value

Elements of EU Added Value for implementing countries authorities included:

- Implementing countries acting alone would unlikely have achieved what the API Directive achieved. The phenomena of irregular migration and terrorism affected implementing countries differently. Implementing countries had different departure points in terms of their adoption of API systems. The Directive provided an impetus without which EU-wide implementation of API systems would probably not have happened. The objectives of the Directive were better served by an intervention at EU level and it had the necessary scale to generate the intended effects.
- The widespread adoption of API systems, the sharing of good practice in EU and international cooperation fora and the use of related processing applications may have helped in implementing countries collectively achieving economies of scale.
- The loss of competence due to EU level action was hence accompanied by benefits that would otherwise would not been generated by implementing countries acting alone.
- The additional benefits of a more homogeneous policy approach are prevented by the fact that the implementation approaches of API systems varied widely across implementing countries
- From a carriers' perspective, the implementation of API systems in the current form has led to limited to no added value. Rather there were missed opportunities which could have generated benefits which in turn could have justified the compliance costs.

In view of the above, it is unlikely that without EU intervention the benefit derived from the implementation of API systems by Member States would have been achieved.

The benefits of the Directive

From the perspective of implementing countries, the implementation of API systems at national level generated the intended benefits. Illustration of specific benefits mentioned by stakeholders are:

- Improved border control and border management:
  - Faster border checks: By running pre-checks against API data on incoming flights, border management authorities can better prepare for conducting first checks and second checks as necessary
  - Faster response to potential irregular migrants and suspected criminals: Border management authorities can identify suspicious passengers before their arrival in the EU and take appropriate measures
  - Faster clearance at the external border: Running pre-checks also allow border management authorities to gain time in processing passengers at the external borders and help reduce waiting times
- Improved migration management:

- Improved risk analyses and better targeting of irregular migrants
- Increased refusal to entry of irregular migrants and capture of facilitators

- Improved law enforcement

  - Better investigation of suspected criminals: Processing passenger data of known suspects revealed important facts which helped investigating related cases
  - Increase in arrest of criminals: Processing of passenger data contributed to numerous arrests, identification of suspects or other previously unknown persons

From the carriers' perspective, the implementation of API systems in the current form has led to limited or to no added value. Industry stakeholders considered that API systems might have facilitated faster clearance of their passenger through the EU external border. Whilst this is a clear benefit for their customer, it is rather indirect and does not outweigh the compliance costs they have incurred. Industry stakeholders pointed missed opportunities in that:

- API systems could lead to the identification of potentially inadmissible passengers before the boarding process – currently there is limited evidence of passengers denied boarding on the basis of API,
- API systems could facilitate passenger travel and avoid additional waiting time at airports,
- Organisational (i.e. multiple authorities in individual Member States requiring API data) and operational requirements (i.e. multiple formats and multiple data elements required across Member States) could be further harmonised to avoid the variations in the way API systems have been implemented.

API in implementing countries in the absence of the Directive

Implementing countries acting alone would have been unlikely able to achieve what the API Directive achieved. The phenomena of irregular migration and terrorism affected implementing countries differently. Implementing countries had different departure points in terms of their adoption of API systems. International Conventions did not mandate API systems until a decade after the transposition deadline of the Directive.

In the absence of EU level action, implementing countries would have had the ability to implement API systems on their own and or under international-level initiatives. At the time of the entry into force of the Directive a few implementing countries were already considering launching advanced passenger information related initiatives (e.g. ES, UK). These implementing countries continued to be at the forefront of the development of API systems in Europe, such as with the introduction of Interactive API system in the UK. Whilst for the most advanced implementing countries the absence of EU level action in the field would not have been detrimental to them implementing API systems, it would not have been the case for these implementing countries that to date have still not yet implemented API systems or have implemented it years after the transposition deadline.

At international level, international cooperation on advance passenger information started in 1993 with the API Guidelines jointly published with WCO and IATA since then regularly augmented by the WCO/IATA/ICAO Guidelines (i.e. in 2003, 2010 and 2013). All implementing countries are contracting parties to the Convention on International Civil Aviation. The new Chapter 9 of the Annex 9 of the Convention on Advance Passenger Information, introduced in 2017, mentions that each State shall establish an

API system and have appropriate legal authority to oblige carriers to comply with standards and recommended practice. Under the international regulatory framework, the objectives pursued by the Directive could have been achieved without said Directive but with, at least, a nine-year delay in the implementation of that framework. The level of compliance of the Contracting Parties with regard to the implementation of API systems and related standards is also unclear at the time of reporting and hence so is the extent to which the Convention would have had the same effects than the Directive.

To implement API systems on their own, implementing countries would have necessitated a consensus on the irregular migration and terrorism related threats they faced to justify the need for API systems. The disparities in terms of incoming flows of irregular migrants across implementing countries existed during the transposition of the API Directive[145] and are still prevalent today[146]. For instance, Spain, France, the United Kingdom, Italy and to a lesser extent Germany have consistently been among the top five EU Member States in terms of the number of irregular migrant refused entry at the border, and especially at the air border.[147] They are also the EU Member States who have been targeted the most by the successful and or foiled terrorist attacks in the last two decades.[148] In those countries the rationale to act would have been greater than in other implementing countries less affected by these phenomena.[149] For instance, Croatia adopted national implementing measures on 1 July 2013 when it acceded to the EU. Its system became fully operational four years after the effective transposition of the Directive.

In this context, the implementation of the Directive helped to establish generic rules and procedures for capturing, transmitting and processing passenger data across implementing countries, although the Directive did not set specific organisational, operational or technological standards.[150] To some extent, EU level action (e.g. the Frontex Advance Information Working Group (AIWG)) as well as EU Member States participation in ICAO Working Groups facilitated the exchange of experience and knowledge on the implementation of API Directive influencing implementing countries' administrations and organisations in adopting similar approaches.

The widespread adoption of API systems, the sharing of good practice in EU and international cooperation fora and the use of related processing applications may have helped in implementing countries collectively achieving economies of scale. If the API Directive had not been adopted and transposed, the cost of implementation of API systems for a limited number of implementing countries and airlines might have been greater[151], as implementing countries might not have benefited from the volume effects brought on by the Directive. The loss of competence due to EU level action was hence

[145] Harmonised data on irregular migration only goes back to 2008 (EUROSTAT).

[146] At EU level, even if (irregular) migration flows have peaked in 2015, they remain at substantially higher levels post 2015 than pre-2015. Similarly, the threat from terrorism continues to be at an all-time high in many Member States (source: Terrorism Situation and Trend Report 2019 (TE-SAT) | Europol).

[147] Eurostat - Third country nationals refused entry at the external borders - annual data (rounded) [migr_eirfs].

[148] ICF elaboration on the basis of SOCTA reports.

[149] This was also commented on in the 2012 evaluation "in some Member States, there was no strong business case to support the implementation of API systems".

[150] The Directive does not set operational or technological standards. Art.6 only provides that API data should be "transmitted electronically or, in case of failure, by any other appropriate means" – no elaboration on the methods of transfer.

[151] Evidence relies on reasoned assumptions and limited qualitative evidence.

accompanied by benefits that would otherwise would not been generated by implementing countries acting alone.

Beside the scale and the volume effects, the phrasing of the obligations of the Directive gave a lot of room for manoeuvre for implementing API systems in a way that fitted implementing countries' needs. Whilst this might have contributed to a swifter adoption of API systems, in the longer term the discretion left to implementing countries to comply with the Directive limited the potential benefits to be derived from its implementation. The implementation section notes a variety of approaches with regard to:

- The data elements collected and incoherent use of data standards and formats
- The procedures for collecting the data
- The scope of the data collection and processing (e.g. carriers' type, specific routes)
- The extent of the processing of the data collected (Some implementing countries process almost 95% of the data collected, others a much lower proportion)
- The level of sanctions and the timing for the imposition of sanctions
- The various operational models put in place by Member States.

The variety of implementation approaches has severely limited the potential EU Added value of the Directive. International and EU level cooperation fora have played a role towards the homogenisation of implementation approaches with introduction of standards and the sharing of good practices.

Despite these limitations, and the fact that some implementing countries are still due to implement API systems, the issues addressed by the Directive still continue to require action at EU level. At EU level, even if migration flows have peaked in 2015, they remain at substantially higher levels in 2019. Similarly, the threat from terrorism continues to be at an all-time high in many EU Member States.[152] In the future, the anticipated evolution of migration flows, terrorism threat, organised crime activities justify the EU level action. For instance, the European Council's new strategic agenda 2019-2024 argues that (1) effective control of the external borders is an absolute prerequisite for guaranteeing security, upholding law and order and (2) there is a need to strengthen our fight against terrorism and cross-border crime. API Data is also now a key component of the border management and internal security acquis (e.g. PNR Directive, Systematic Checks).

In view of the above, it is unlikely that without EU intervention the benefit derived from the implementation of API systems by implementing countries would have been achieved.

[152] Source: Terrorism Situation and Trend Report 2019 (TE-SAT) | Europol).

6. CONCLUSIONS

This section provides the conclusions of the evaluation, summarising the findings and highlighting which elements of the EU intervention are working or not and why; analysing the lessons learned and assessing if issues need to be addressed by action or will resolve over time.

Evaluation findings

Relevance

The rationale for collecting API data is still valid 15 years after the entry into force of the API Directive. The objectives of the API Directive (i.e. border control management, combating against irregular migration, law enforcement including fighting terrorism) remain highly pertinent to the needs of the relevant stakeholders and the wider societies. In addition, collecting API data is also relevant to facilitate legitimate travel which is currently not per se an objective of the Directive.

The professionalisation and internationalisation of terrorist and organised crime groups and their cross-border activities, together with international calls for an increased use of API data, suggest that in the future this instrument will be even more relevant to support implementing countries in facing new challenges.

Effectiveness

The implementation of API systems has overall been effective for border control purposes, to tackle irregular migration and for internal security purposes including fighting terrorism and serious and organised crime. By accessing information on passengers in advance, border authorities benefit from additional time for analysis, the management of border crossing points is optimised and second-line response by national authorities is more effective.

However, the lack of harmonisation in the implementation of the Directive is an obstacle to its effectiveness.

Efficiency

National authorities perceived that the overall costs incurred from the implementation of API systems have been proportionate and are justified, considering the extent of resources used and the nature and level of benefits and impacts achieved to date, while carriers considered that the costs incurred from the implementation of API systems are only partially or not at all justified, given that (direct) benefits have been minimal for them.

Coherence

The objectives of the national API systems are compliant with the objectives of the API Directive. However, as a result of the "minimum requirements" imposed by the Directive, the implementation of API systems and the actual usage of API data show a fragmented picture. In addition, the option left to implementing countries to collect and use API data for law enforcement purposes, without providing a clear definition of this purpose nor laying down a framework for processing data, led to a disjointed implementation at national level.

As concerns coherence with other EU instruments, similar (almost identical) set of personal data will be captured, transmitted and processed for purposes of carrier's query into ETIAS/EES/(VIS). There are several discrepancies between the API Directive and the EU PNR Directive causing operational challenges in practice and uncertainty for data subjects. Moreover, the data protection requirements are not in line with the most recent developments in the field.

In addition, the API Directive is not fully coherent with the international regulatory framework on passenger information, especially as concerns data fields and transmission standards.

EU added value

It is unlikely that without EU intervention the benefits derived from the implementation of API systems by implementing countries would have been achieved. The Directive provided an impetus without which EU-wide implementation of API systems would probably not have happened. The objectives of the Directive were better served by an intervention at EU level as it had the necessary scale to generate the intended effects.

The issues addressed by the Directive still continue to require action at EU level.

Lessons learned

The evaluation process highlighted a number of shortcomings related to the API Directive. These elements affect the impact of the Directive, create burden on the stakeholders and generate a certain level of legal uncertainty, both for the entities collecting and transmitting the data, for the authorities processing them, and ultimately for the data subjects.

Lack of standardisation

Currently there are a number of areas where lack of standardisation and harmonisation lead to reduce the benefits of the whole processing of API data.

From a **governance and organisational perspective**, the API Directive does not mandate specific organisational structures or responsible authorities (except for authorities responsible for border controls) to perform the obligations mandated in it. This creates an administrative burden for carriers as they need to understand each national organisational model in order to transmit API data to the relevant national – and in some cases sub-national – authorities in each individual implementing countries. In addition carriers are in some cases obliged to send the same data to different authorities. This would not be the case if a "single window approach" was developed, i.e. if single national authorities or a single European authority were mandated to collect all data coming from carriers, or if a centralised routing mechanism was set up to receive all the data and transfer them to relevant authorities.

In addition to the above, the API Directive does not mandate specific roles or the delineation of responsibilities necessary for the functioning of API systems, thus creating different governance arrangements at national level, including different – in some cases insufficient – oversight measures or mechanisms to be in place to ensure compliance of API systems with data protection requirements.

As regards the **scope and extent of API data collection**, there is a great variety across implementing countries in terms of types of flights; types of routes; types of carriers as well as transport modes (i.e. air, waterborne, land). In addition, the number and type of

data elements required by responsible authorities also vary across implementing countries. Article 3(2) of API Directive provides a non-exhaustive list of data elements and the list mentioned in it is not in line with international standards (especially as regards the collection of API data from the MRZ).

According to national authorities this heterogeneity is likely to create security loopholes as gaps in coverage are likely to be exploited by serious and organised crime organisations and or terrorist organisations.

In addition, the **operational procedures** for capturing, transmitting, processing and analysing API data vary in their methods, timing, format, frequency of transmission across implementing countries:

- On data capture: data collection through online booking systems or through manual data entry at the check-in is a widespread practice which can result in poor quality of API[153], while technological solutions are currently available to verify API data via a scan of the MRZ, or even reading authenticated data from a chip, including and especially for online check-in[154];
- On the timing of data transmission: implementing countries request the transmission of API data at several points in time (eight implementing countries receive API data more than once)[155]. The Directive requires API data transmission 'by the end of check-in' (Art 3(1)); this is not considered sufficiently precise as passengers may, exceptionally, be added after formal closure of check-in.[156]
- On the format and method of data transmission: The API Directive allows data transmission 'electronically or, in case of failure, by any other appropriate means' (Art 6(1)). It does not mandate a specific messaging protocol and format. This results in additional burden for carriers (e.g. in complying with the varied format required by responsible authorities to transmit data) but has also an effect on the timeliness and quality of the API data and hence impacts its usefulness.

Overall, a more automated and streamlined collection and transmission of the data would lead to, on one hand, less quality issues and, on the other hand, a more efficient and fully automated quality process, contributing to the reduction of time invested in interaction with carriers.

Lack of data protection safeguards

While the processing of personal data within the scope of the API Directive (for border control purposes) falls within the general legal framework foreseen by the GDPR, the API Directive does not itself provide for detailed safeguards for the protection of personal data with the exception of Article 6(1) which provides that, for border control and migration purposes, authorities shall delete API data within 24 hours after transmission.[157] In contrast to the API Directive, more recent legal instruments, such as EES (Chapter VII Art 51-59), ETIAS (Chapter XII Data protection Art. 59-70) and PNR (Art. 12 and 13) include more detailed provisions on inter alia the periods for retaining

[153] On routes operated by low-cost carriers, an industry average of 50% of passenger do not use check-in desks since they only carry hand luggage (source: Evaluation Study).

[154] Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information and Passenger Name Records https://op.europa.eu/en/publication-detail/-/publication/3ce76d7a-2838-11e9-8d04-01aa75ed71a1/language-en

[155] This is against Recommended Practice 9.10 listed in Annex 9 of Chicago Convention.

[156] Source: Evaluation Study.

[157] Unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders.

the data, the deletion of data, and the obligation to depersonalise data. Thus, there is scope for further clarification of this aspect in the API Directive.

In summary, the current state of play presents several challenges:

- The list of API data elements required from air carriers is not exhaustive which is against the principle of data minimisation.
- The purpose of API data collection (border control and/or law enforcement purposes) is unclear; this has led to inconsistent processing of API data throughout implementing countries with possible unlawful processing of personal data according to data protection legislation.
- The more requests for API for different purposes and multiple 'pushes' of API data to competent authorities at different points in time (as part of API Directive and of the PNR Directive), the more instances of unnecessary data collection and processing, again against the principle of data minimisation.
- For border control purposes, the 24-hour data retention limit may be too short for long haul flights or for flights with connections and no transfer. Likewise, 24 hours may be too short in case of deficient quality or unstructured format of the data transmitted.
- The obligation to delete data within 24 hours after transmission "unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders" is not sufficiently defined and not accompanied by the clear rules on data retention and subsequent use.
- There is a lack of data protection oversight mechanisms (e.g. data protection officer, regular reporting on the access and processing of personal data) however these obligations apply to API authorities as of 2018 as established by the GDPR .

This results in legal uncertainty and potential breaches of data protection legislation.

Lack of clarity

The numerous coherence issues observed showed that the Directive is currently not aligned with the latest policy and legal developments at EU level in the area of integrated border management, internal security and data protection.

The Advance Passenger Information ecosystem has evolved significantly since the adoption of the API Directive in 2006:

- The PNR Directive mandates the transfer of API data, if collected by the carriers for their own purposes, to be processed with PNR data for the purposes of law enforcement;
- The Systematic Checks Regulation mentions the possibility to carry advanced checks on the basis of API data;
- The future entry into force of the EES and ETIAS (and probable VIS recast) will require pre-travel authorisation, collection of biographic data for third country nationals and an obligation to query the systems by carriers, that favoured the use of the ICAO industry standard " iAPI" for querying these systems.
- The international community mandated standards and encouraged the use of API data for counter terrorism purposes.
- The new data protection framework (GDPR and Law Enforcement Directive) came into force.

In addition to the coherence with other legislative instruments, two internal inconsistency have been observed:

1) The use of API data for law enforcement purposes, including fight against organised crime and terrorism, is not clearly defined in the Directive thus creating uncertainty on how API data should be collected, transmitted and processed for this purpose.
2) The geographical scope suffers from a lack of clarity, as the notion of "third country" as defined in the Directive leaves room for interpretation.

All these elements play a role, or will do so in the near future, on how API data is collected and processed and should therefore be integrated in the general framework regulating API data as they are unlikely to solve over time.

ANNEX I: PROCEDURAL INFORMATION

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

The Evaluation Roadmap for the initiative was published by DG Migration and Home Affairs (DG HOME) on the Commission's 'Have your say' webpage in December 2018. The Terms of Reference for engaging a contractor to carry out the external study as part of the evaluation were drawn up and a contractor selected in early 2019. The study commenced on 1 March 2019 and ended on 28 February 2020. The agenda planning (Decide) reference assigned to the evaluation is PLAN/2018/4573.

DG HOME unit B1 "Borders and Schengen" was in charge of the Evaluation until 15/9/2019; from 16/9/2019 onwards the file was transferred to DG HOME unit D1 "Police cooperation and information exchange".

2. ORGANISATION AND TIMING

As per the Better Regulation Guidelines, an inter-service steering group was set up within the Commission to oversee the evaluation. Several Directorates-General (DGs) within the Commission[158] were invited to nominate representatives to the steering group.
The meetings of the steering group were chaired by DG Migration and Home Affairs (HOME). The steering group was regularly consulted over the course of the evaluation, typically in conjunction with the submission of specific draft reports by the contractor responsible for carrying out the external study. These consultations took place both in the context of regular meetings, via email and telephone. The following list provides an overview of the steering group's work over the course of the evaluation:
The inter-service steering group (ISSG) was convened for the first time on 16 November 2018 in order to receive initial information about and provide feedback on draft versions of the Terms of Reference for the external study and the Stakeholder Consultation Strategy, which described how the Commission intended to consult with different stakeholder groups in the context of the evaluation; The ISSG met with the contractor on 24 June 2019 and on 6 September 2019; the draft final report was received on 16 December 2019. A meeting of the ISSG with the contractor took place on 16 January 2020 and the final report of the study was accepted on 28 February 2020.
The steering group was consulted during the drafting of this staff working document.
The evaluation was extended, given the fact that the public consultation was launched later than initially anticipated for technical reasons (The Public Consultation was online from 10/9/2019 until 3/12/2019).
This decision was made out of respect for the Better Regulation Guidelines and in order to allow the contractor adequate time to account for all responses to the Consultation.

[158] Secretariat General, Legal Service, DG MOVE, DG TAXUD, DG JUST.

3. EXCEPTIONS TO THE BETTER REGULATION GUIDELINES

In conducting the evaluation, no exceptions from the usual procedural requirements described in the Better Regulation Guidelines were required.

4. CONSULTATION OF THE RSB (IF APPLICABLE)

Not applicable.

5. EVIDENCE, SOURCES AND QUALITY

Most of the evidence was collected with the support of an external contractor (see "Study on evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 – Final Report, March 2020) via national research, desk research, stakeholder consultations (including Public Consultation) and industry e-survey.

Limitations were mitigated as follows:

- 1) Comprehensive primary data collection and analysis compensated for the lack of a substantial body of literature
- 2) Support via Permanent Representations to facilitate contacts with stakeholders in implementing countries
- 3) Where quantitative data was not available, alternative proxy data or qualitative evidence was provided in the analysis
- 4) Approximations and assumptions where data was not available have been clearly outlined.

ANNEX II: SYNOPSIS REPORT OF THE STAKEHOLDER CONSULTATION

1. CONSULTATION STRATEGY

The goal of the consultation strategy was to ensure that, across a series of consultation activities, all relevant stakeholders at EU, national and international level were given an opportunity to express their views on the functioning of the API Directive. The consultation strategy relied on a mix of methods and tools to ensure a comprehensive and representative collection of views and experience with the functioning of the Directive. The tools and methods used were complementary in that they allowed to reach out to all concerned stakeholders, including:

- Public Consultation: open to the general public (self-selection);
- Stakeholder interviews at EU, international and national level;
- Industry survey: targeted to carriers and other industry players.

This strategy, mostly implemented in the framework of the Evaluation Study, was complemented by informal meetings with representatives of the two main stakeholders group (national authorities and carriers, including IATA), and visits to API centres in Bulgaria, France and Germany.

In addition to the above, the evaluation roadmap was published and remained open for comments by stakeholders for four weeks. Comments received were integrated in the subsequent analysis.

The outcomes of this additional consultations were in line with the results outlined in the Evaluation Study.

2. METHODOLOGY

This section elaborates on the methodology of the stakeholder consultation.

2.1. PUBLIC CONSULTATION (PC)

The Public Consultation (PC) was launched on 10 September online on EU Survey platform and was opened until 3 December 2019 (duration of 12 weeks). As a common practice, the PC was available in all EU official languages.[159] All stakeholders and the general public had the possibility to provide their views and inputs as part of a public consultation.

A total number of 42 responses were received from a range of stakeholders. The results of the PC are analysed in a separate Annex to the Evaluation Study (Final Report, March 2020).

[159] Except Irish (Gaelic).

2.2. TARGETED INTERVIEWS

Targeted interviews at EU and international level

To ensure a balanced representation of views, a number of stakeholders at EU and international level were consulted via face-to-face or phone interviews. Overall, the interviews have been conducted as planned. A total of 35 interviews have been carried out by the evaluation team as presented in Table 1.

Table 1. Overview of interviews at EU and international level

Stakeholder type	Stakeholders interviewed	# Interviews
1.EU institutions and agencies	• DG HOME (3 interviews) • DG MOVE • DG JUST • EBCGA (group interview) • FRA (group interview) • Eu-LISA • Europol • European Data Protection Supervisor • Representatives from European Parliament, LIBE Committee • Counter-Terrorism Coordinator	• 12 interviews carried out
2.International and European industry associations	• International Air Transport Association (IATA) • Airlines for Europe (A4E) • Airlines International Representation in Europe (AIRE) • Association of European Airlines (AEA) • International Road Transport Union (IRU) •	• 5 interviews carried out • Industry survey (32 respondents)
3. International and European organisations	• International Organisation for Migration (IOM) • Organization for Security and Co-operation in Europe (OSCE) • International Maritime Organisation (IMO) • Airpol[160] • ICAO • World Customs Organisation	• 6 interviews carried out
4.Passenger associations and NGOs	• European Passengers' Federation (EPF) • Access Now •	• 2 interviews carried out

[160] A law Enforcement Network created to build synergies for police and border guard units working in the fight against crime in the European aviation sector, https://www.airpoleuropa.eu/.

Stakeholder type	Stakeholders interviewed	# Interviews
5.Technological solutions providers	• Société Internationale de Télécommunications Aéronautiques (SITA) • Amadeus	• 2 interviews carried out • Industry survey
6. Air carriers	• Lufthansa • Swiss • Norwegian • Ryanair • Easyjet • Qatar Airways • Brussels Airlines • Condor (former Thomas Cook)	• 8 interviews carried out • Industry survey •
7. Land and waterborne carriers	• Royal Caribbean Cruises LTD (RCL) • Community of European Railway and Infrastructure Companies (CER) • Eurostar	• 3 interviews carried out •

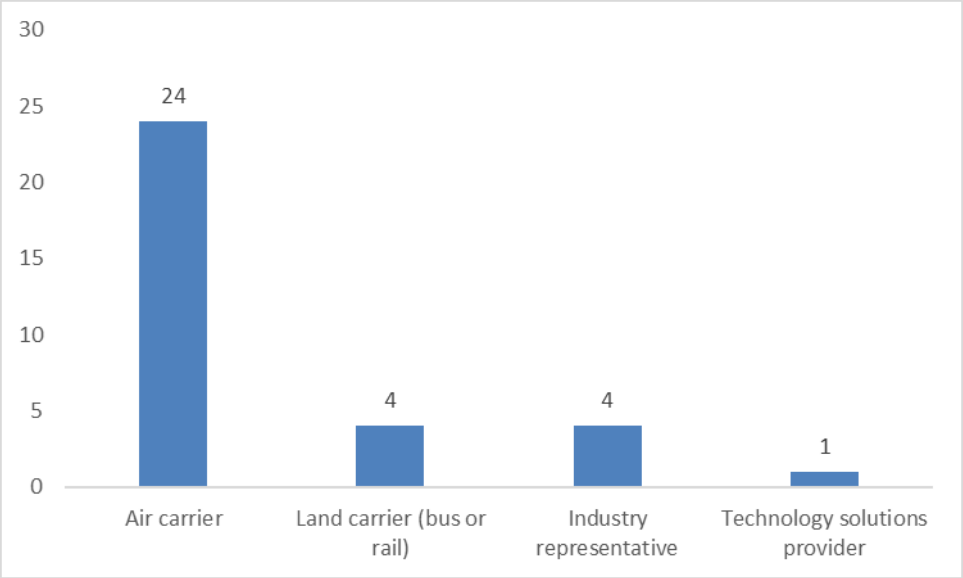
Interviews at national level

Stakeholder interviews with competent national authorities were carried out in all of the 31 implementing countries, including with Ministries of Interior, border management authorities, data protection authorities and other competent authorities – depending on the organisational set-up in the country.

Industry survey

The industry survey was launched on 11 June 2019 and was live for 4 weeks. The International Air Transport Association (IATA) and the Airlines International Representation in Europe (AIRE) were actively involved in its dissemination among their members. Industry organisations for other modes of transport have also been invited to participate in the survey and to further distribute the survey among their members. A total number of 33 stakeholders have provided complete responses. The total number of incomplete responses was 67; however, we have considered in the analysis only the 33 completed responses to ensure quality (e.g. avoid duplicates). As shown in Figure 3, from the 33 responses, 24 were air carries; 4 land carriers; 4 industry representatives and one technology provider. Amongst the air carriers were some of the largest carriers in Europe and globally (including national carriers) as well as low cost carriers.

Figure 1. Respondent types to the industry survey



2.3. RESULTS OF THE STAKEHOLDER CONSULTATIONS

This section presents a summary of the results of the stakeholder consultation by evaluation criterion.

Relevance

Interviews with implementing countries authorities indicated that implementing countries clearly see a need for collecting API data. According to representatives of national authorities, collecting API data is necessary for passenger pre-checks because border authorities would know the identities of the individuals prior to arriving in the implementing country. By obtaining the data beforehand (as soon as the passengers have boarded the aircraft at the airport of departure), border guards have time to examine whether there are passengers on board who are on watchlist or those who are not allowed to enter the country and would require secondary checks at arrival. In this sense, API is seen as an important tool for facilitating border control as it allows for faster clearance of passengers.

A number of **EU level stakeholders and industry stakeholders** expressed the view that the intended objectives of the API Directive could not be fully pursued due to the low level of harmonisation leading to an uneven implementation. Implementing countries have implemented API systems differently and some implementing countries are more advanced in terms of their technical capabilities than others.

Overall, the majority of **industry survey** respondents believed that the collection and transmission of API data has helped address the needs. About 70% of all respondents (total no. 32 respondents), strongly agreed or agreed that API has helped improve border control and about 60% believed that API has contributed to combatting irregular migration.

This is less so when it comes to combatting terrorism (43% of respondents agreed or strongly agreed); fighting transnational crime (40% of respondents agreed or strongly

agreed) and enhancing internal security and public order (38% of respondents agreed or strongly agreed).

Reasons given by respondents for disagreeing with the above statements were:

- Scepticism whether data is fully utilised prior to the arrival of passengers
- Countries not working properly with API data to fulfil objectives
- Implementing countries not using interactive API: iAPI is more effective to stop illegal migration, as it prevents the person from boarding the aircraft
- The ease with which criminals are believed to be able to obtain fraudulent documentation

With regard to responses to the **Public Consultation (PC)**:

- 85% of respondents strongly agreed or agreed API Directive is relevant to enhancing internal security;
- 83% of respondents strongly agreed or agreed API Directive is relevant to improving border control;
- 78% of respondents strongly agreed or agreed API Directive is relevant to fighting terrorism;
- 75% of the respondents strongly agreed or agreed API Directive is relevant for combatting irregular migration.

The majority of respondents to the PC (55% or 21 responses) reported that in their view the objectives of the EU policy on API could be better achieved through other means, as opposed to 45% (or 17 responses) of respondents that reported the objective could not be better achieved. 4 out of 11 respondents reported that the objectives of the EU policy on API could be better achieved through merging the API and PNR Directives so that responsible authorities can use better instruments to combat crime. In addition, 2 respondents revealed that the objectives could be better achieved if the scope of data collection is extended to include other types of transport in addition to air transport. Another 2 respondents reported that this could be achieved through the introduction of an interactive API system. One respondent underlined that there should be less responsibilities for air carriers, specifying that a uniformed system of all border controls in EU should be linked to carriers' systems. Finally, 1 respondent specified that the objectives could be achieved by traditional intelligence services and border surveillance and another one reported that they could be achieved through operative information exchange between relevant authorities.

Effectiveness

Interviews with **national stakeholders** revealed that the API Directive has been overall effective in achieving its objectives of improving border control and combatting irregular migration. The interviewees highlighted benefits such as improved time to conduct border checks and overall facilitation of border control, as well as the possibility of identifying passengers in advance and the improved targeting of irregular migrants. The national stakeholder interviews also revealed that the use of API data for law enforcement has enhanced internal security and public order, as well as other benefits mentioned such as improved risk analyses, better targeting and use of resources. The main factors impeding the objectives of the Directive that were identified during the interviews were the low quality of API data in some implementing countries, as well as the difficult negotiations with carriers. Finally, national stakeholders reported that the automatic capture of API data decreases the possibility of errors and data collected from

the machine-readable zone of the travel document contains fewer mistakes. It was also revealed that technical development issues in the context of the API data is an ongoing process that should be addressed.

During the interviews with **carriers** it was reported that overall API systems have been effective in improving border control and combatting irregular migration. Respondents revealed that the effectiveness of API systems in the area of law enforcement has been limited, with some of them reporting insufficient visibility on the topic. In addition, carrier interviews acknowledged that possible obstacle to the achievement of the objectives of the API Directive is the limited cooperation between industry and authorities. Finally, it was reported that the API Directive has negatively impacted carriers because of the costs for implementing the technical solutions to collect API data, as well as the sanctions resulting from untimely or wrongful transmission of passenger data. This was also confirmed during the interviews with EU institutions and agencies, which revealed that the API Directive has unfavourably impacted carriers.

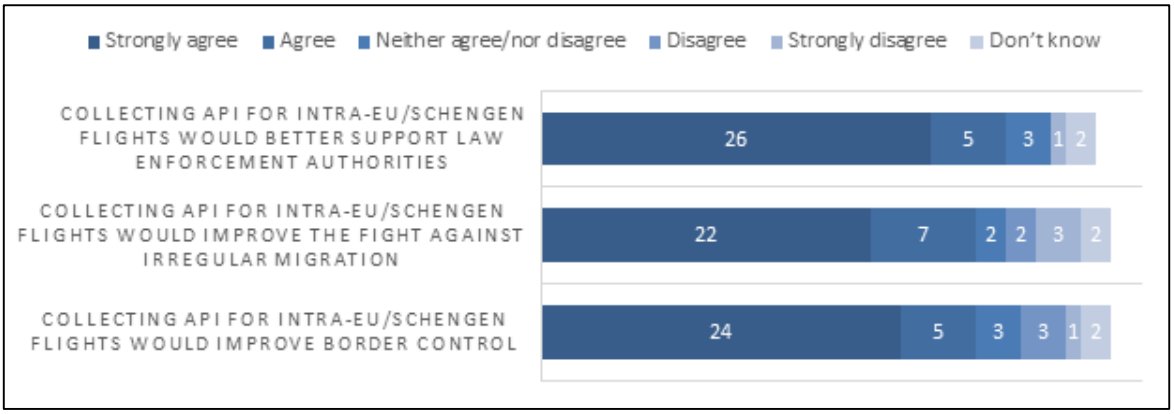
EU and international stakeholders interviewed have mentioned that the wording of the Directive may have a negative impact on the effectiveness of the Directive in improving border controls, with examples given the lack of clear and harmonised list of data criteria.

The interviews with **industry associations** have highlighted as a positive contribution to the objectives of the Directive the relationships built with key stakeholders within government agencies which has allowed for discussion on technological improvements in the area.

The **industry survey** revealed that for the majority of respondents the main improvements that have taken place as a result of the implementation of API are the reduced exposure to penalties for carriers, the better identification of high-risk passengers and the better screening of inbound and outbound passengers. Other benefits identified were the reduced costs associated with removal of persons, the reduced staff costs because of automation, as well as the reduction of waiting times for passengers. The industry survey also indicated that the main impacts of implementing API are on law enforcement authorities and carriers, with limited impact noticed for passengers.

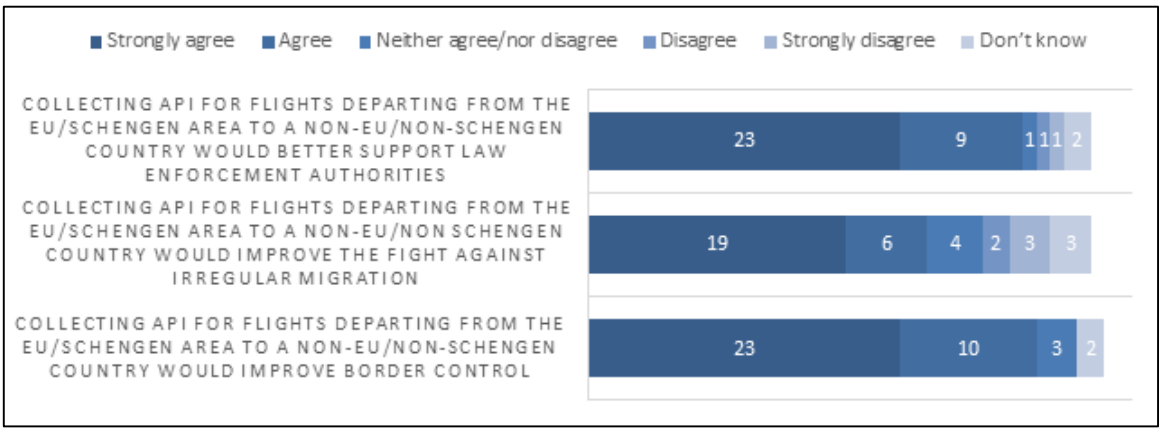
A large majority of respondents to the **PC** either strongly agree or agree that collecting API for intra-EU/Schengen flights would improve border control, improve the fight against irregular migration and would better support law enforcement authorities. As can be seen in Figure 1, respondents that either strongly disagree or disagree to these statements account for a minority of responses.

Figure 1. Do you agree collecting API for intra-EU/Schengen flights would improve the following?



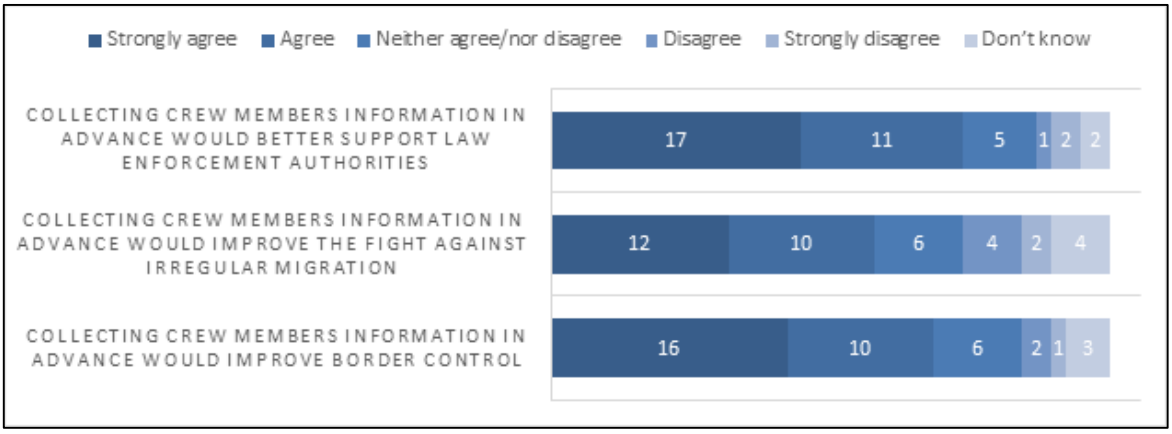
As can be seen in Figure 2, a large majority of respondents to the **PC** either strongly agree or agree that collecting API for flights departing from the EU/Schengen area to a non-EU/non-Schengen country would improve border control and the fight against irregular migration, as well as would better support law enforcement authorities. On the contrary, respondents that disagree or strongly disagree account for a fraction of responses.

Figure 2. Do you agree collecting API for flights departing from the EU/Schengen area to a non-EU/non-Schengen country would improve the following?



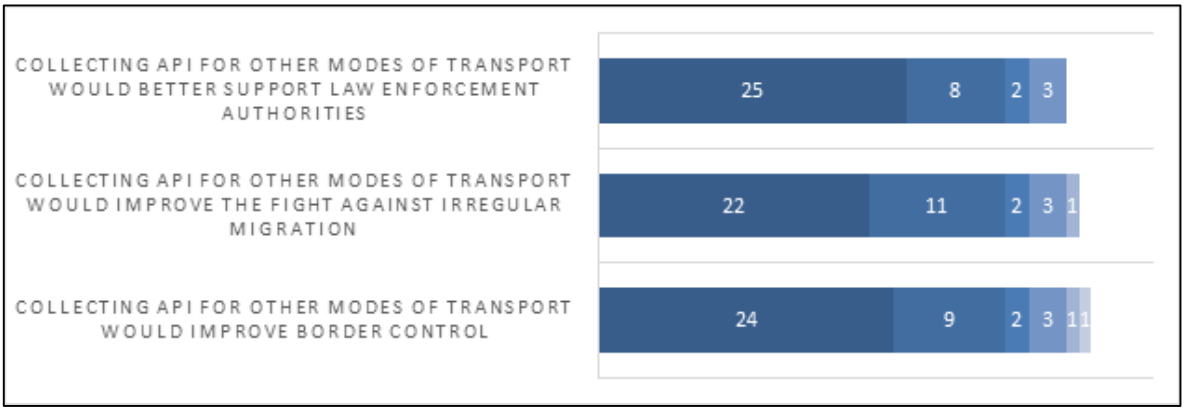
As can be seen in Figure 3 below, a large majority of respondents to the PC either strongly agree or agree that collecting crew members information in advance would improve border control and the fight against irregular migration, as well as would better support law enforcement authorities. Respondents that either disagree or disagree to these statements account for a minority of responses.

Figure 3. Do you agree that collecting crew members information in advance would improve the following?



As can be seen in Figure 4, a large majority of respondents to the **PC** either strongly agree or agree that collecting API for other modes of transport would improve border control and the fight against irregular migration, as well as would better support law enforcement authorities. On the contrary, respondents that disagree or strongly disagree account for a fraction of responses.

Figure 4. Do you agree collecting API for other modes of transport would improve the following?



Efficiency

National authorities perceived that the overall costs incurred from the implementation of API systems have been proportionate and are justified, considering the extent of resources used and the nature and level of benefits / impacts achieved to date.

Most **air carriers** interviewed as part of this research viewed the implementation of their respective API system as having been "burdensome," owing to the extent of resources involved in their set-up and maintenance. A few air carriers also discussed "unforeseen costs," notably financial penalties resulting from non-compliance. In that regard, however, concerns were raised in relation to procedures surrounding the imposition of financial sanctions. A few carriers felt that sanctions were often inflicted with no clear indication of how the API data gathered and shared did not meet the necessary requirements.

A large majority of respondents to the **PC** reported that they do consider that the implementation of API has brought benefits (80% or 32 responses), as opposed to 3% (or 1 response) of respondents that reported that they do not consider this. In addition, 17% (or 7 responses) of respondents reported that they do not know.

A large majority of respondents (85% or 29 responses) identified support to law enforcement authorities as the main benefit of the implementation of API. This was followed by the benefit of better identification of irregular migration (82% or 28 responses) and the benefit of faster border checks (65% or 22 responses). Finally, only 3% (or 1 response) of respondents reported that there are other benefits from the implementation of API.

Coherence

Interviews with **border control authorities** revealed that representatives from ten Member States perceive that the objectives of their national API systems are fully aligned with those of the API Directive – combatting irregular migration and improving border control. In addition, border control representatives from three Member States reported that their national API systems are also collected for law enforcement purposes and to fight against terrorism. Similarly, to border control authorities, the majority of respondents from interviews with Ministry and Targeting Centre representatives reported that they perceive the objectives of their national API systems are fully aligned with those of the Directive.

Interviews with **EU institution representatives** highlighted that most challenges found during the first evaluation of the Directive are still topical in 2019. As the Directive is a pre-TFEU instrument in the area of Justice and Home Affairs, the transposition was left to the interpretation of the Member States. To a certain extent, the definitions and concepts included in (or absent from) the API Directive are not entirely in line with those used in more recent instruments adopted by the EU in border management. Additionally, as stated by another EU institution representative (1) given the margin of interpretation left by the Directive to Member States, the implementation varies: for some, collecting API data is purely a border management issue, while for others it is a law enforcement issue. Leaving a wide margin of interpretation regarding the implementation of the Directive eventually puts into question the standards for border control – as well as security – in the Schengen area.

To the **PC** question "*To what extent do you agree/disagree that the policy on API defined at EU level is better able to achieve objectives to improve border control, combat irregular migration and support law enforcement authorities than if defined at national/regional level?*", out of 42 respondents, a large majority of respondents either strongly agree (51% or 21 responses) or agree (27% or 11 responses) that the EU policy on API is better able to achieve objectives to improve border control, combat irregular migration and support law enforcement authorities than if defined at national/regional level. In addition, 17% (or 7 responses) of respondents neither agree nor disagree, as opposed to 5% (or 2 responses) that do not know.

To the question *"The EU has adopted a new legal framework on data protection (a General Data Protection Regulation (GDPR) – Regulation 2016/679 and a Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes – Directive 2016/680) which protects persons with regard to the processing of their personal data. Against this background, to what extent do you agree/disagree that the EU measures on API are coherent with that legal framework?",* out of a total of 40 respondents, respondents that strongly agree or agree that the EU measures on API are coherent with the legal framework on data protection account for 20% (or 8 responses) and 35% (or 14 responses) respectively, while those that neither agree nor disagree account for 25% (or 10 responses). In addition, respondents that disagree and strongly disagree account for 3% (or 1 response) and 5% (or 2 responses) respectively. Finally, respondents that reported they do not know account for 12% (or 5 responses). Additionally, 2 of them highlighted that it should be taken in consideration that some aspects of the use of API data for law enforcement purposes could be problematic. In addition, 2 respondents reported that the low quality of API data could be a potential issue concerning data protection

To the question, "*Please indicate, if any, other pieces of EU legislation interacting with the EU policy on API. Please briefly explain.",* out of 10 respondents, 6 respondents reported that other pieces of EU legislation that interact with the EU policy on API include the Entry Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). In addition, 2 respondents mentioned interaction of API with the Schengen Border Code. 1 respondent reported that the PNR Directive and the IMO-FAL[161] obligations also interact with API and another mentioned the Treaty of Amsterdam.

EU added value

Interviews with **national stakeholders** revealed that the main added value from the implementation of the API Directive has been observed in the harmonisation of practices in relation to API across implementing countries, as well as in the enhanced cooperation between responsible national authorities and carriers. Another added value that was identified during the national stakeholder interviews was the use of API data for the purposes of detecting terrorism and other crime activities. In addition, a number of representatives from implementing countries have reported that a good practice that emerged from the Directive was the automation of the passenger data collection, transmission and analysis processes.

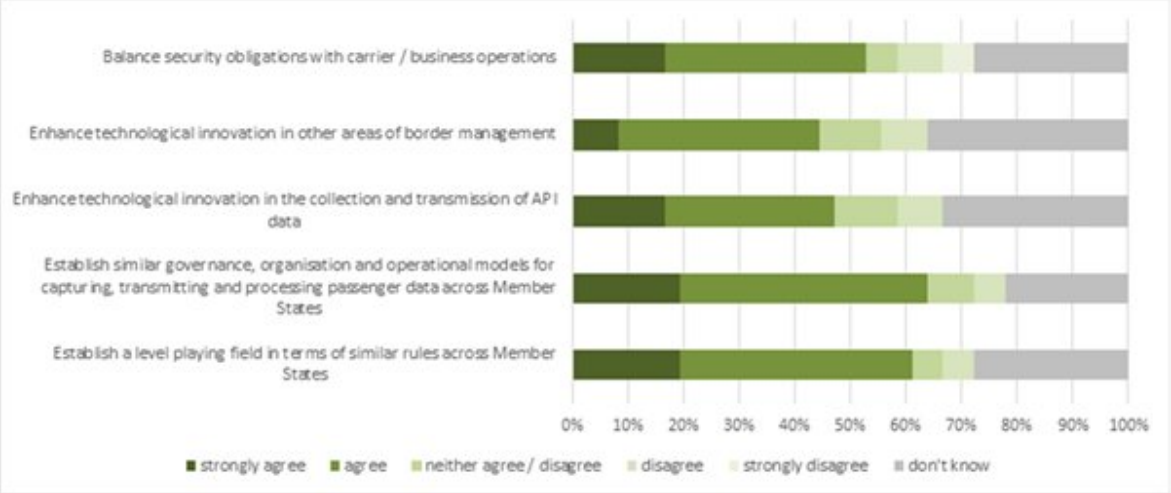
[161] International Maritime Organisation - Facilitation of International Maritime Traffic.

The interviews with representatives from **carriers** revealed that the added value of API systems in implementing countries is limited according to the stakeholders. The main benefits of implementing API were identified to be the harmonisation of legislation on the EU level, which has provided guidance to implementing countries concerning API systems, as well as the establishment of a working group of experts and authorities.

While stakeholders from **industry associations** reported that the EU added value of the API Directive has been in the harmonisation and standardisation that it brings to the area of passenger data, interviews with EU institutions and agencies revealed that there has not been sufficient harmonisation on the EU level.

Overall, the main added value of the API Directive for respondents to the **Industry survey** has been in establishing similar governance, organisation and operational models for capturing, transmitting and processing passenger data across implementing countries. Another added value that was identified by respondents to the industry survey was the establishment of a level playing field in terms of similar rules across implementing countries. However, less than 50 per cent of the Industry survey respondents find that the Directive brings added value in enhancing technological innovations in the collection and transmission of API data or in other areas of border management.

Figure 5. In your view, what is the added value of the EU policy and legislation on API and its implementation, over and above what could have been achieved by Member States alone?



Respondents to the **PC** revealed that the main added value of the EU policy on API has been in bringing harmonisation of legislation and standardisation of data collected across implementing countries, as well as in enforcing implementation of API systems in countries. Other prominent benefits that were identified by respondents were the exchange of information between responsible authorities in implementing countries, as well as the overall increased security in the EU. In addition, it was acknowledged that even though the API Directive has limitations, issues would have occurred if Member States were acting on their own.

ANNEX III: METHODS AND ANALYTICAL TOOLS

In this annex, the methodology applied for the evaluation are described, as well as the limitations that were encountered.

Most of the methodological steps of this evaluation were carried out with the support of an external contractor who reported on their findings and recommendations in their study on evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 – Final Report, March 2020. The results of the report were discussed and analysed by the API evaluation Inter-Service Steering Group and lead to the conclusions highlighted in this paper.

The methodological steps followed were the following :

1) **Inception:** ensure understanding between the external contractor and the Inter-Service Steering Group, agree on objectives and timing, carry out initial desk review and consultations, develop data collection tools and risk mitigation strategy.
2) **Data collection and stakeholder consultations:** establish the baseline of the analysis, carry out national research, desk research, stakeholder consultations (including Public Consultation) and industry e-survey.
3) **Analysis**: assess and compile the results of research, surveys and consultations, evaluate and assess findings and discuss them at an expert workshop.
4) **Synthesis**: conclude on the results of the evaluation study, considering other inputs coming from stakeholders, and develop conclusions on each evaluation criterion.

Step 1: Inception

The purpose of the Inception stage was to lay down solid foundations for the subsequent stages of the evaluation. The main deliverables under this task was the Inception Report. The inception phase was fully completed on 16 May 2019.

Step 2: Data collection and stakeholder consultation

The purpose of Step 2 was to carry out comprehensive primary and secondary data collection and stakeholder consultations which fed into the analysis.

The main deliverables under this task were the First Interim Report, presenting the baseline and contextual analysis, preliminary results of the stakeholder consultation; updated methodological tools and problems and limitations log and mitigation measures, finalised on 2nd July 2019 and the second Interim Report presenting preliminary findings of the evaluation based on the legal and implementation research carried out in Member States until August 2019 finalised on 20th September 2019.

This step consisted of different types of research each presented below with its limitations and mitigating factors:

Desk research

The desk research comprised of a comprehensive review of existing sources at EU, international and national level. A list of sources of information and literature is presented in annex 5.

Limitations:

- Although an extensive review of academic and grey literature was carried out, overall the body of literature on the topic was limited. There were few articles focusing specifically on API systems and the API Directive. A large number of articles have been published on PNR, particularly on data protection, privacy and fundamental rights which also included some information on API (although mostly tangentially and not as the primary focus).
- As the API Directive was adopted in 2004 (pre-Lisbon Treaty and with no opinion from the European Parliament or an impact assessment), few documents specifically focusing on the API Directive were available (e.g. such as opinions issued by relevant stakeholders).
- The bulk of documents examined were legislative and policy documents which provided a solid knowledge base of the API Directive within the broader passenger information landscape. However, limited 'evaluative' evidence (i.e. evidence on what works well, desirable outcomes, etc.) was available from the literature (see above also on lack of published opinions).

Mitigation measures:

- Because of the lack of secondary data, the evaluation included a comprehensive primary data collection and analysis which compensated for the lack of a substantial body of literature.
- The national research carried out in all Member States applying the API Directive helped form a solid basis for the evaluation.
- A comprehensive stakeholder consultation with 10 stakeholder types facilitated the creation of 'evaluative' evidence.

Legal and practical implementation of the API Directive at national level

This exercise aimed to provide an up-to-date view of the (i) state of legal transposition and (ii) practical implementation in the 31 implementing countries.

National researchers for each implementing country have been appointed at the beginning of the evaluation. They were tasked with literature review, assessment of the national implementing measures, interviews with key officials and quantitative data collection.

Limitations:

- Limited secondary sources (desk research) were available at national level.
- Initial difficulties in reaching relevant stakeholders were experienced in some country. However, at least one competent authority has been consulted in each of the 31 implementing countries, with certain type of authorities being more responsive and active to answer interview requests (e.g. PIUs) which also depended on the administrative organisation established.

- Quantitative data (such as on number of hits and budgetary data) was not readily available in all implementing countries.
- Due to the wide scope of the evaluation (covering a detailed list of implementation questions as well as evaluation questions), not all topics may have been fully covered during the face-to-face interviews with national authorities.

Mitigation measures:

- In instances where limited national sources were available, the study team aimed to carry more extensive primary data collection (i.e. where possible to carry out further interviews).
- Reminders and requests to participate in the evaluation to Member States via the Permanent Representations.
- Efforts have been made to find additional contacts via researcher's network of contacts at national level.
- Where not all aspects have been covered during an interview, the study team requested additional information to be sent via email.
- Where quantitative data is not available, the study team either provided alternative proxy data or where this is also lacking, made this explicit in the analysis and supplemented the analysis with qualitative evidence.

Public consultation

The Public Consultation (PC) was launched on 10th of September online on EU Survey platform and was opened until 3rd December 2019 (duration of 12 weeks). As a common practice, the PC was available in all EU official languages.[162] All stakeholders and the general public had the possibility to provide their views and inputs as part of a public consultation. A total number of 42 responses were received from a range of stakeholder types. The results of the PC are analysed in a separate Annex (Annex 2 to this report) as well as integrated into the evidence base for the evaluation.

No significant limitations have been encountered concerning the PC.

Although respondents to the PC were not were numerous and represented mainly the same stakeholder types to those consulted already through other means (e.g. industry survey and interviews), the information collected was useful for complementing the already collected information and to have an overall larger sample of responses.

Targeted consultations

Targeted consultations at EU and international level

A total of 38 interviews have been carried out by the evaluation team as presented in Table 1.

Table 1- Overview of interviews at EU and international level

[162] Except Irish (Gaelic).

Stakeholder type	Stakeholders interviewed	# Interviews
1.EU institutions and agencies	• DG HOME (3 interviews) • DG MOVE • DG JUST • EBCGA (group interview) • FRA (group interview) • Eu-LISA • Europol • European Data Protection Supervisor • Representatives from European Parliament, LIBE Committee • Counter-Terrorism Coordinator	• 12 interviews carried out
2.International and European industry associations	• International Air Transport Association (IATA) • Airlines for Europe (A4E) • Airlines International Representation in Europe (AIRE) • Association of European Airlines (AEA) • International Road Transport Union (IRU)	• 5 interviews carried out • Industry survey (32 respondents)
3. International and European organisations	• International Organisation for Migration (IOM) • Organization for Security and Co-operation in Europe (OSCE) • International Maritime Organisation (IMO) • Airpol[163] • ICAO • World Customs Organisation	• 6 interviews carried out
4.Passenger associations and NGOs	• European Passengers' Federation (EPF) • Access Now	• 2 interviews carried out
5.Technological solutions providers	• Société Internationale de Télécommunications Aéronautiques (SITA) • Amadeus	• 2 interviews carried out • Industry survey
6. Air carriers	• Lufthansa • Swiss • Norwegian • Ryanair • Easyjet • Qatar Airways • Brussels Airlines • Condor (former Thomas Cook)	• 8 interviews carried out • Industry survey
7. Land and waterborne carriers	• Royal Caribbean Cruises LTD (RCL) • Community of European Railway and Infrastructure Companies (CER) • Eurostar	• 3 interviews carried out

[163] A law Enforcement Network created to build synergies for police and border guard units working in the fight against crime in the European aviation sector, https://www.airpoleuropa.eu./

No significant limitations have been encountered concerning EU and international level interviews. The vast majority of the interviews have been completed and have provided good quality primary evidence for answering the evaluation questions.

As expected, some stakeholders have provided more details on some aspects than others. The level of details in the responses differs across stakeholder types, depending on their competencies.

Industry survey

The industry survey was launched on 11 June 2019 and was live for 4 weeks. The International Air Transport Association (IATA) and the Airlines International Representation in Europe (AIRE) were actively involved in its dissemination among their members. Industry organisations for other modes of transport have also been invited to participate in the survey and to further distribute the survey among their members. A total number of 33 stakeholders have provided complete responses. The total number of incomplete responses was 67; however, the study team considered in the analysis only the 33 completed responses to ensure quality (e.g. avoid duplicates). From the 33 responses, 24 were air carries; 4 land carriers; 4 industry representatives and one technology provider. Amongst the air carriers were some of the largest carriers in Europe and globally (including national carriers) as well as low cost carriers.

No significant limitations have been encountered concerning the industry survey, in particular thanks to IATA and A4E who disseminated the survey to their members. In comparison, the 2012 evaluation received only 6 responses from air carriers. A higher level of engagement was achieved this time through cooperation with the industry stakeholders.

Step 3: Analysis

The following tasks were undertaken as part of the Analysis phase:

- Assessing the quality of the transposition of the API Directive
- Analysing the implementation activities
- Carrying out a thorough evaluation and analysis of the findings
- Drafting of Issue paper
- Discussing and developing best practice and recommendations

An expert workshop was carried out on 28th November 2019 with 19 participants in order to contextualise and confirm the findings and conclusions of the evaluation with the experts.

Limitations:

- Limited quantitative data received from national authorities (including cost data, and data on results, such as number of hits)

Mitigation measures:

- Where quantitative data is not available, alternative proxy data were provided or where this is also lacking, this was made explicit in the analysis and supplemented with qualitative evidence.
- Approximations and assumptions where data is not available have been clearly outlined.

Step 4: Synthesis and Reporting

The following tasks are were undertaken in the last phase of the project:

- Present the evidence with regard to the quality of the transposition and implementation of the API Directive;
- Conclude on the conformity of the Directive's transposition in Member States' legal framework;
- Conclude on the relevance – coherence, effectiveness, impact and added value of the Directive;
- Conclude on best practices in view of the main issues identified

The main deliverable under this task was the Final Evaluation Report, finalised on 28 February 2020, which constitutes the basis of this Staff Working Document.

No significant limitations have been identified in relation to this final phase

ANNEX IV: EVALUATION CRITERIA AND QUESTIONS

In accordance with the Commission's Better Regulation Guidelines, the evaluation's overall objective was to assess the relevance, coherence, effectiveness, efficiency, EU added value and sustainability of the Directive as applied in all implementing countries. In achieving this objective, a number of specific evaluation questions related to the different evaluation criteria were developed and appear below.

Evaluation questions on **relevance**:

- *To what extent are the objectives of the Directive pertinent to the needs, problems and issues the Directive is aiming to address?*
- *To what extent do the intended benefits of the national API systems respond to the needs, problems and issues as identified at national level? Are the objectives of the Directive relevant to the national needs?*
- *Is the API data collected, transmitted and used in line with data protection requirements?*

Evaluation questions on **coherence**:

- *How do the provisions of the API Directive and API systems operate together to achieve its objectives?*
- *To what extent are the obligations under the API Directive coherent with other obligations under EU legislation in the same policy field?*
- *To what extent is the API Directive coherent with the international regulatory framework on passenger information?*

Evaluation questions on **effectiveness**:

- *To what extent has the Directive achieved its objectives and corresponding intended impact on improving border controls?*
- *To what extent has the Directive achieved its objectives and corresponding intended impact on combating irregular migration issues in Member States/EU?*
- *To what extent has the Directive achieved its objectives and corresponding intended impact on enhancing Internal security and public order as well as fight against terrorism?*
- *What factors have contributed to or impeded the intended objectives of the Directive?*
- *To what extent has the Directive achieved its intended impact among key groups?*

Evaluation questions on **efficiency**:

- *To what extent are resources being efficiently used in achieving the intended impact of the Directive?*
- *What are the costs and the benefits of the Directive?*

- *What have been the costs related to the practical implementation of API systems for Member States' carriers?*
- *What are the operating costs of running API systems for Member State authorities and carriers?*
- *To what extent are the results, outcomes and impacts achieved at a reasonable cost?*
- *Are there measures to reduce possible unnecessary burdens, which do not undermine the Directive's objectives?*

Evaluation questions on **EU added value**:

- *What has been the added value of implementing API systems for Member States and carriers?*
- *Could the objectives of the policy have been achieved sufficiently by the Member States acting alone?*
- *Could the objectives of the proposed action be better achieved at Union level by reason of the scale or effects of that action?*

ANNEX V – LIST OF SOURCES

Policy proposals and communications

- A4E, IATA Feedback on the Roadmap for the Evaluation of the API Directive 2004/82/EC
- 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
- Evaluation Roadmap for Advance Passenger Information (API) Directive
- Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
- Proposal for a Regulation of the European Parliament and of the Council on the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
- Proposal for a Regulation of the European Parliament and of the Council concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
- Commission Communication to the council and the European Parliament Preparing the next steps in border management in the European Union
- Commission Communication to the council and the European Parliament Preparing the next steps in border management in the European Union
- Consultations of December 2006 as part of the IA Proposal for a COUNCIL FRAMEWORK DECISION on the use of Passenger Name Record (PNR) for law enforcement purposes
- Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003 COM (2003) 826.
- OSCE Ministerial Council Decision 6/16 of December 2016 Enhancing the use of Advance Passenger Information
- G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism, 26-27 May 2017
- National impact assessments on API and response to European Commission Consultation

Legislative documents

- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (API Directive)
- Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985

- 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 (PNR Directive)
- Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders
- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES)
- Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS)
- Regulation (EU) 2016/399 of the European Parliament and of the Council on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)
- Regulation 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 (General Data Protection Regulation – GDPR)
- Directive 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 (Law Enforcement Directive)
- 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
- Convention on International Civil Aviation (Chicago Convention)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
- United Nations Security Council Resolution 2178/ (2014)
- United Nations Security Council Resolution 2309 (2016)
- United Nations Security Council Resolution 2396 (2017)
- United Nations Security Council Resolution 2482 (2019)
- Member State's national acts, laws and regulations

Opinions

- FRA Opinion 2/2018, The revised Visa Information System and its fundamental rights implications (2018)
- Recommendation 1/98 on Airline Computerised Reservation Systems (CRS), 28 April 1998, WP 10 (Art. 29 Data Protection Working Party)
- Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, 19 January 2005, WP 103 (Art. 29 Data Protection Working Party)
- Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data, 27 September 2006, WP 127, (Art. 29 Data Protection Working Party)

- Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (Art. 29 Data Protection Working Party)
- Opinion 1/15 of the Court of Justice of the European Union of 26 July 2017 on the draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data
- On the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record Data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (European Data Protection Supervisor – EDPS)

Official reports

- Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82, 2012
- Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information and Passenger Name Records
- Frontex Report on API Systems and Targeting Centres
- Fundamental rights at airports: Border checks at five international airports in the European Union, FRA 2014
- Under watchful eyes: Biometrics, EU IT systems and fundamental rights, FRA 2018
- Guidelines on Advance Passenger Information (API), WCO/IATA/ICAO, March 2003
- Guidelines on Advance Passenger Information (API), WCO/IATA/ICAO, March 2010
- Guidelines on Advance Passenger Information (API), WCO/IATA/ICAO, 2013
- Guidelines on Advance Passenger Information (API) WCAO/IATA/ICAO, 2014
- Code of Practice on the management of information shared by the Border and Immigration Agency, Her Majesty's Revenue and Customs and the Police, UK Home Office – 2006
- Harmonisation of Advance Passenger Information (API) regimes, *ICAO*, 31/03/2008
- Harmonisation of advance passenger information requirements, ICAO, 14/02/2008
- ICAO/WCO/IATA Management Summary on Passenger-related Information
- ICAO Doc. 9303 on Machine-Readable Travel Documents
- Recommendations relating to ICAO's Best Practices relating to Passenger Name Records (PNR), 31/09/2008
- Report from the United Nations Counter-Terrorism Executive Directorate on Gaps in the use of advance passenger information and recommendations for expanding its use to stem the flow of foreign terrorist fighters, 26 May 2015
- Advance Passenger Information (API), European Civil Aviation Conference, 20/03/2008
- European Migration Network Reports
- European Commission, Technical Study on Smart Borders, Final Report 2014

- OSCE, Overview of Advance Passenger Information (API) in the OSCE Area, 2017
- UK Home Office, second report on statistics being collected under the exit checks programme, August 2017

Other literature and statistical sources

- Eurostat statistics
- Eurobarometer surveys on data protection
- Eurocontrol statistics on the basis of CFMU IFR Flights and Eurocontrol Annual report
- Eu-Lisa, SIS II 2017 Statistics
- IATA statistics, ICAO statistics
- Study on ways of setting up an EU network on exchange of Passenger Name Record (PNR) data for law enforcement purposes "Accenture and SITA" – 2009
- the World Trade Organisation (WTO) forecast: Tourism 2020 vision,
- The travel forecast of Office of Travel and Tourism Industries (OTTI),
- DG ENTRE – Admin Burden Reduction Website
- National Administrative Burden Reduction Websites
- EC, PNR Factsheet: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en
- EC, Smart Border Factsheet https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en
- EUObserver, "Private jets- the Achilles heel of EU air traffic security?", 27/07/2018,: https://euobserver.com/justice/142472
- DG HOME Glossary: Push method
- DG HOME, Glossary, SIS II, https://ec.europa.eu/home-affairs/content/second-generation-schengen-information-system-sis-ii_en
- DG HOME Glossary: Visa Information System (VIS)
- DG HOME, https://ec.europa.eu/home-affairs/e-library/documents/policies_en?policy=442
- DG HOME, Alerts and data in the SIS, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/alerts-and-data-in-the-sis_en
- DG HOME, Prevention of and Fight against Crime (ISEC), https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime_en
- DG HOME, Internal Security Fund – Police
- EMN Glossary: Advance passenger information (API)
- EMN Glossary: Border control
- EMN Glossary: Border crossing point
- EMN Glossary: Entry/Exit System (EES)
- EMN Glossary: European Travel Information and Authorisation System (ETIAS)
- EMN Glossary: European integrated border management
- EMN Glossary: Irregular migration
- EMN Glossary: Schengen Information System (SIS)
- EMN Glossary: Third-country national
- Interpol, Stolen and Lost Travel Documents database

- CNEWS, “Arrestations Ratees: La Faute a Cheops, le Fichier de la Police?”, 24.09.2014 https://www.cnews.fr/france/2014-09-24/arrestations-ratees-la-faute-cheops-le-fichier-de-la-police-691918
- Centre de crise, BelPIU, https://centredecrise.be/nl/inhoud/belpiu-collection-and-processing-passenger-data
- International Civil Aviation Organization (ICAO), Working Paper, facilitation Panel, 9th Meeting, Montreal, 4-7 April, Agenda Item 3: Amendements to Annex 9, Advance Passenger Information
- ICAO, Third Interregional Aviation Security and Facilitation Seminar 13-15 October 2018, Cairo
- ICAO Glossary

Law journals

- European Journal of Migration and Law
- DPLoW = Data Protection Laws of the World. Published by Sweet and Maxwell
- The Journal of air law and commerce
- Revue française de droit aérien et spatial
- Zeitschrift fuer Luftrecht und Weltraumrechtsfragen

Official journals and legislative databases

- Official Journals of The Member States of The European Union
- EUR-LEX Legislation Online