EUROPEAN
COMMISSION

Strasbourg, 13.12.2022
SWD(2022) 422 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the documents

Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC

Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818

{COM(2022) 729 final} - {SEC(2022) 444 final} - {SWD(2022) 421 final} - {SWD(2022) 423 final}

Table of contents

Glossary

Term or acronym	Meaning or definition
API	Advance Passenger Information
CJEU	Court of Justice of the European Union
CRM	Centralised Routing Mechanism
EES	Entry / Exit System
ETIAS	European Travel Information and Authorisation System
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
iAPI	Interactive API
ICAO	International Civil Aviation Organization
IATA	International Air Transport Association (IATA)
LED	Law Enforcement Directive
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OSCE	Organisation for Security and Cooperation in Europe
PAXLST	Passenger List Message
PIU	Passenger Information Unit
PNR	Passenger Name Record
SARPs	ICAO Standard and Recommended Practices
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents database (Interpol)
VIS	Visa Information System
WCO	World Customs Organization
UNSCR	United Nations Security Council Resolution

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

The last decades have witnessed an **increase of people travelling by air**. In 2019, the International Civil Aviation Organisation (ICAO) reported 4.5 billion passengers globally carried by air transport on scheduled services.[1] The **EU recorded about 1 billion passengers** in the same year, 520 million flying from or to extra-EU countries, 335 million on intra-EU flights and 160 million on domestic flights.[2] After a temporary decline due to COVID-19 related travel restrictions, the volume of passengers is expected to continue to increase in the coming years.

An **effective management of the Schengen external borders** is a prerequisite to enhancing security in an area without border controls within the EU. It requires Member States to apply firm and uniform criteria on the controls on entry and exit at the Schengen external borders. **All travellers**, meaning third-country nationals, stateless persons and EU citizens crossing the Schengen external borders, are to be **effectively and systematically checked** against the relevant databases[3]. To achieve this goal, the Schengen Borders Code was amended in 2016 and 2017.[4]

The fact that over half a billion passengers enter or leave the EU every year puts **a strain on the external air borders of the EU**. To ensure that systematic checks can be efficiently performed on every air passenger,[5] there is a need to **speed up** border controls at airports and ensure the **facilitation** of passenger flows while at the same time maintaining a high level of security.

The processing of **Advanced Passenger Information** (API) is an effective tool for border authorities to anticipate their workload and to perform adequate border controls. API informs competent authorities in advance of the volume and identity of air travellers, allowing for **pre-checks of air travellers** prior to their arrival at the external border. API is a set of information on passengers such as name, date-of-birth, passport details, attributed seat, the baggage details and the exact travel route, that air carriers collect during check-in (either online check-in or check-in at the airport) and transmit in advance (at departure of the plane) to competent authorities of the country of destination. The sources of this information are the passenger's travel document and the boarding card.

As first-line border guards are under time pressure to perform their checks on air passengers, the availability of API greatly facilitates their tasks. It allows border officials located in a back office to query API data against databases such as the Schengen Information System (SIS), Interpol systems and national databases and watchlists well in advance of the actual arrival of the passenger. In doing so, persons of interest can be identified in a timely manner, and relevant information can be passed on to first-line border guards for further follow-up upon arrival of the passenger Consequently, effective external

---

[1] ICAO, The World of Air Transport in 2019, https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx.
[2] Source: Eurostat (online data code: avia_paoc) ; these figures include the passenger transport in all current EU Member States (27 Member States).
[3] As recalled most recently in the Joint statement by the EU home affairs ministers on the recent terrorist attacks in Europe, 13 November 2020; and by the European Council, Conclusions of 10 and 11 December 2020, EUCO 22/20.
[4] As per Article 8 of Regulation (EU) 2016/399 (Schengen Borders Code), amended Regulation (EU) 2017/458, border checks on persons includes checks against the SIS, Interpol's Stolen and Lost Travel Document (SLTD) database, and national databases.
[5] European Commission, State of Schengen Report 2022, COM(2022) 301 final/2, 24.5.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0301.

border management requires that every person is pre-checked with API data ahead of the arrival at the external borders.

At international level, the **Convention on International Civil Aviation** (Chicago Convention[6]) stipulates that each State shall establish an API system and have appropriate legal authority to oblige carriers to comply with the related standards and recommended practices as adopted by ICAO.

At EU level, the 2004 **API Directive** regulates the transmission of API data to Member States to improve external border controls.[7] The Directive imposes an obligation on air carriers to transmit API data, upon request, to the border authorities of the country of destination prior to the flight's take-off. The API Directive is without prejudice to Member States using API data also for law enforcement purposes – which constitutes a separate purpose distinct from border management – in accordance with national law.[8]

The API Directive was evaluated in 2020 to assess the transposition by Member States and set up of national systems to collect and use API data.[9] That evaluation assessing the **implementation of the API Directive** showed that all Member States have transposed the API Directive and most[10] have implemented systems to collect and use API data. The 2020 evaluation also found that the API Directive remained pertinent with regards to the objectives pursued, namely border management and the fight against irregular migration. It however noted limitations in the implementation of the Directive. The lack of legal precision provided by the Directive has resulted in a plethora of national interpretations, creating gaps in the collection and use of API data and therefore undermining the overall effectiveness of the Directive. The evaluation also indicated that due to differences in the use of API data for border management and law enforcement as two distinct purposes with different operational needs, the effective use of API data for law enforcement purposes would require a dedicated legal instrument.

There is indeed a global consensus that API data is not only a key instrument for border management, but also an **important tool for law enforcement purposes**, notably to **counter serious crime and terrorism**.[11] The 2020 evaluation set out that the processing of API data for law enforcement including terrorism is highly pertinent. At international level, since 2014, **United Nations' Security Council** Resolutions have repeatedly called for the establishment and global roll-out of API systems for law enforcement purposes.[12]

Criminals make frequent use of the EU's main airports as well as smaller regional airports operating low-cost airlines.[13] Their capability to travel fast and long distance, by air, without being detected (notably within the EU), has become an essential modus operandus for cross border criminality. The same applies for terrorism, with most terrorist campaigns having a

---

[6] Chicago Convention or Convention on International Civil Aviation adopted in 1944, which established the International Civil Aviation Organisation (ICAO). All Member States are parties to the Chicago Convention. ICAO Convention on International Civil Aviation; See also 2014 WCO/IATA/ICAO Guidelines on Advance Passenger Information

[7] Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data ('API Directive').

[8] Article 6 of API Directive.

[9] An evaluation was completed in 2020: European Commission, Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 8 September 2020, SWD(2020) 174.

[10] With the exception of Greece and Cyprus.

[11] Europol, Serious and Organised Crime Threat Assessment (SOCTA), 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

[12] UN Security Council Resolution 2178(2014), 2309(2016), 2396(2017), 2482(2019), as well as OSCE Ministerial Council Decision 6/16 of 9 December 2016 on Enhancing the use of Advance Passenger Information.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

transnational character, with the involvement of cross-border contacts or travels outside the EU. In this latter context, preventing foreign terrorist fighters (FTFs) from travelling to the EU and returning from conflict zones remains a particular priority.[14] In traveling to and from conflict zones, FTFs often resort to indirect or '**broken travel**' routes that combine different type of itineraries, outside and within the EU. The analysis of air passenger data has proven crucial for preventing departures and detecting the return of FTFs.[15]

As shown by the report on the Passenger Name Record (PNR) Directive review, **the joint processing of API and PNR data** plays a vital role in identifying, preventing, detecting, and disrupting terrorism and other serious crimes,[16] as it enables the confirmation of identity of travellers and greatly improves the reliability of PNR data (*see Box 1 below*).[17] However, the current EU legal framework only regulates the collection of PNR data for fighting serious crime and terrorism but does not do so for API data, leading to a security gap notably with regard to intra-EU and domestic flights. Addressing this gap, the June 2021 strategy towards a **fully functioning and resilient Schengen area** called for an increased use of API data in combination with PNR data for intra-Schengen flights to significantly enhance internal security, in compliance with the fundamental right to the **protection of personal data** and the fundamental right to **freedom of movement**.[18]

Box 1: Advanced Passenger Information and Passenger Name Records

Passenger data are usually composed of two types of data: Advance Passenger Information (API) and Passenger Name Records (PNR).

When a passenger buys a ticket with an air carrier, a **PNR** will be generated by the reservation systems of air carriers. This includes some but not all personal data, but also the **complete itinerary, payment details, contact-details and special requests** of the passenger. This PNR data is sent to the Passenger Information Unit (PIU) of the country of destination and often the country of departure.

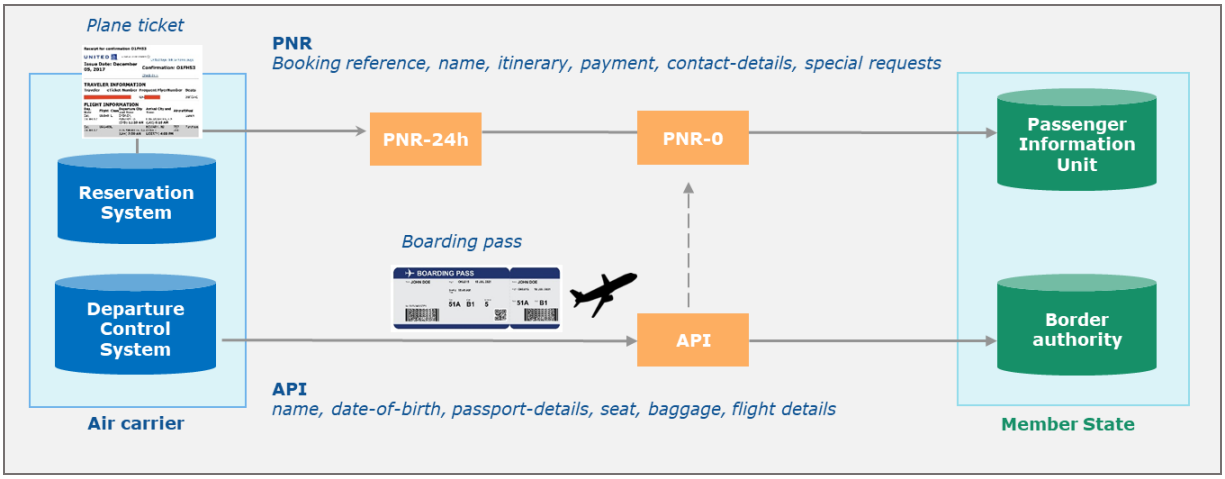
API data is captured by the air carrier during **check-in** of the passenger (online check-in and at the airport). This data is stored in the carrier's Departure Control System (DCS) and generally sent to competent border authorities as a complete 'passenger list manifest' containing all passengers on board (so called batch-API delivery) at departure of the plane.

Both API and PNR contain information pertaining to the passenger and the flight on which he or she will arrive or depart. Both the PNR data and the API data contain a common reference (a six character booking reference) to enable **consolidation** of both data sets and therefore **combined processing**.

While, API data are considered as **'verified'** information as it corresponds to information on the travel document, and which can also be used by law enforcement authorities in order to identify suspects and persons sought, PNR data is **unverified** information provided by passengers. The PNR data of a certain passenger usually do not contain all potential PNR elements, but only those actually provided by the passenger and/or necessary for the booking.

Figure 1 Collection and transfer of API and PNR data to Member States' authorities

[14] Europol, Terrorim Situation and Trend Report, 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf
[15] Consultations with Member State experts for the purpose of this impact assessment.
[16] European Commission, Staff Working Document Accompanying the Report on the review of Directive 2016/681, SWD(2020)128 final, p. 43
[17] SWD(2020)128 final, p. 43.
[18] COM(2021) 277 final (2.6.2021).



2. PROBLEM DEFINITION

The 2020 evaluation of the API Directive,[19] and the consultation process carried out for the purposes of this impact assessment,[20] have revealed a number of **gaps and inconsistencies in the way Member States process API data** both for border management and for law enforcement purposes. These gaps and inconsistencies can be clustered into **two main problems**: The first problem concerns shortcomings in the use of API for pre-checks of persons before they cross the Schengen external borders. The second problem relates to the suboptimal use of API data for law enforcement purposes and the security gaps this creates. The following table presents **the main problems and underlying drivers**.

Table 1: Overview of the problem and their drivers

Problems	Drivers
Not every person crossing the Schengen external borders is pre-checked with API data	1. No obligation on Member States' authorities to request API data from carriers, not aligned with international obligations regarding the establishment of API systems 2. Inconsistent practices in Member States driven by the design of the legal provisions, in particular: • No clear criteria on which **flights** API data should be collected • Non-exhaustive list of **data fields** to be collected, not aligned with international standards on API (WCO/IATA/ICAO API Guidelines) • No specification of the **method** to collect API data
There are security gaps in the processing of air passenger data for law enforcement purposes	– Security gap regarding flights where only PNR data is collected (i.e. not on intra-EU and domestic flights) – No clear EU rules on the use of API for law enforcement purposes, particularly on the retention period of the data, data elements and flight coverage, leading to uneven safeguards in terms of passengers' protection of personal data

[19] European Commission, Directorate-General for Migration and Home Affairs, Study on Advance Passenger Information (API): evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, Publications Office, 2020, https://data.europa.eu/doi/10.2837/882434.

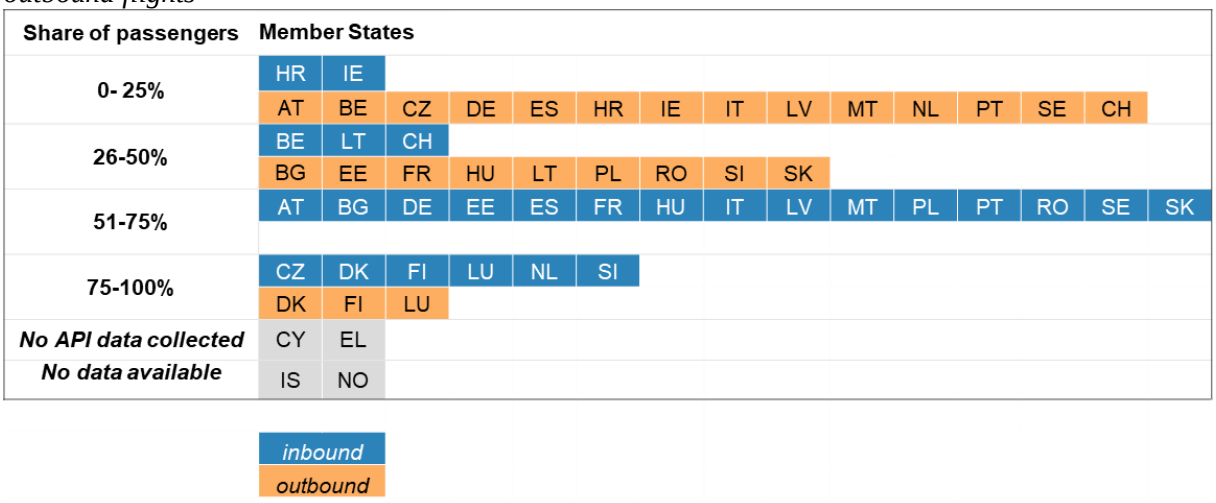
[20] For details on the stakeholder consultation, see Annex 2.

2.1. Not every person crossing the Schengen external border is pre-checked with API data

2.1.1. What is the problem?

The API Directive is a tool supporting the application of the Schengen Borders Code by making external border checks more efficient. Effective external border management requires that every person is pre-checked with API data ahead of the arrival at the Schengen external borders. While the 2020 evaluation of the API Directive observed that Member States have implemented national API systems, it also observed that **Member States make insufficient use of the possibility of API data processing to enhance border management**. The way the API Directive is implemented by Member States varies greatly, driven by the flexibility that the Directive's requirements provide.[21] As a consequence, not every person crossing the Schengen external border is pre-checked with API data. The percentage of passengers for which API is collected and used as a tool for border management varies substantially amongst Member States. At aggregated level, for all Member States combined, this figure is estimated at 65% for inbound flights. In addition, there is an estimated use of API data for 25 % of all outbound flights for law enforcement purposes under national law.

Chart 1: Member States and share of passengers on whom API data is collected on inbound and outbound flights



Source: Data gathered from surveys sent to national authorities for the preparation of the external study supporting an impact assessment: Potential effects of different possible measures on advance passenger information and collected in autumn 2020.

This patchwork of flight coverage creates a situation where it is easy for individuals that want to avoid checks to bypass routes where API data is consistently collected and instead fly and enter the Schengen area via travel routes where API data is less or not used.

Once transmitted by air carriers, API data enables border guards to perform pre-checks on the identity of passengers and the validity of the travel document used against the databases provided for in the Schengen Borders Code.[22] The Schengen Borders Code indicates that border checks on persons must be performed by checking the information contained in the

[21] European Commission, Evaluation of the API Directive, SWD(2020)174, 8.9.2020, p 13 onwards.
[22] Article 8(2)(a) of the Schengen Borders Code refers to the SIS, Interpol's Stolen and Lost Travel Documents (SLTD) database, and national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

travel document against relevant international (Interpol's SLTD, EU (Schengen Information system) and national databases, also on the basis of advance passenger data.[23]

To add to the problem, the 2020 evaluation also demonstrated that when and where API data *is* collected by Member States, their national authorities do not use the API data in a consistent way to ensure effective external border management. For example, not all Member States use the API data for pre-checks against the databases set out in the Schengen Borders Code.[24]

Finally, there is a data quality issue. An effective use of API data requires the data to be **accurate and complete**. If identity data is not reliable and verified, which sometimes is not the case today, cross-checks in databases will not yield reliable operational results. The collection and transmission of API data is should be aligned with international API data standards[25] to would ensure compliance of the API requirements by the air industry.

2.1.2. What are the problem drivers?

This problem is driven by **differences in the approaches of the Member States towards the collection and processing of API data**. There is no legal obligation on Member States to request and use API data.[26] The flexibility left to national authorities for the collection and processing of API data led to divergent practices, where a few Member States collect API data systematically while others do not. This is the main driver of passengers not being pre-checked with API data ahead of their arrival at the Schengen external borders.

The API Directive only puts the **obligation *on carriers* to transmit API data *if* requested by Member States**. However, while all Member States have legally transposed the Directive, not all Member States have taken measures to request air carriers to transmit API data. Two Member States have not even set up a national system for the collection and use of API data.[27] In a context where the API Directive leaves it to the discretion of Member States whether or not to request API data, no infringement procedures could be initiated to enforce the processing of API data.

Moreover, even where Member States make use of the possibility under the API Directive to request air carriers to transmit API data, the Directive sets only **limited criteria** for the collection, transmission and processing of API data as regards the flight coverage for the collection of data, the data elements to be collected, or the means to capture the data. This leads to **very diverging practices**.

Firstly, **flight coverage varies among Member States**, as the API Directive does not indicate the scope of flights for which API data should be collected. The Directive offers the **possibility** to request API data on flights crossing the external borders without providing any guidance or criteria on how to select the flights for the collection of API data.[28] Only a few Member States

[23] Article 8(2)(e) of the Schengen Borders Code.
[24] See European Commission, Directorate-General for Migration and Home Affairs, Study on Advance Passenger Information (API) : evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, Publications Office, 2020, https://data.europa.eu/doi/10.2837/882434, p. 149
[25] WCO/IATA/ICAO Guidelines on Advanced Passenger Information (API), 2014. See Annex 5.
[26] Article 3(1) of the API Directive.
[27] Cyprus and Greece have not yet a fully implemented API system.
[28] Article 3(1) of the Directive provides that Member States shall take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out *checks on persons at external borders*, by the end of check-in, information

collect API data on all flights from third countries (see Chart 1 above). The majority of Member States collect data on selected flights only, in most cases covering over 50% of the passengers but in some cases only a small percentage. Several Member States also request API data from carriers departing to third countries for law enforcement purposes. This patchwork of flight coverage creates a situation where it is easy for individuals that want to avoid checks to bypass routes where API data is consistently collected and instead fly and enter the Schengen area via travel routes where API data is less or not used.

Secondly, the API Directive includes a mandatory but **non-exhaustive list of API data fields** covering passenger data and flight information.[29] While these elements are mandatory, Member States can request additional data fields in line with national legislation. Most Member States make use of this possibility.[30] This in turn represents an **additional burden on air carriers** that need to comply with a different set of requirements depending on the routes on which they transport passengers and the Member State requesting data. Particularly on this point, industry stakeholders stressed the need for a future API instrument to take into account **the evolutions in the international guidelines concerning API data collection** since the adoption of the Directive, as developed in ICAO, the International Air Transport Association (IATA) and the World Custom Organisation (WCO) API guidelines (see Annex 5).[31]

Thirdly, as **online check-in became a common practice** in the past 20 years, API data from a travel document is increasingly manually transcribed or "self-declared" by passengers.[32] This can **lead to incomplete or incorrect data transmitted to national authorities** (e.g. misspellings in the surname and last names, use of the automatic pre-filling function of forms leading to errors). Incomplete or erroneous API data can create **loopholes in the depth and type of checks** that national authorities can perform, **negatively affecting the time needed to carry out checks in databases** (e.g. more resources needed to manually review the results of automated checks).

Incomplete or erroneous API data can **impact passengers** because of **'false-positive' automatic matches**. Good quality data, both in the query as well as in the database, leads to exact matches that prevents passengers from being subjected to incorrect, unnecessary interviews. Where API data is incomplete (e.g. missing date-of-birth, missing gender, missing travel document number) or incorrect (misspelled name, mix-up of numbers), it may lead to matches that may need to be confirmed or inferred by physical secondary checks on the person and the travel document.

The need to ensure that API data collected is accurate and complete is closely linked to the means or methods used by airlines to ensure that API data collected corresponds to the information displayed on travel documents. The API Directive does not prescribe **the means**

---

concerning the passengers they will carry *to an authorised border crossing point through which these persons will enter the territory of a Member State*. See also SWD(2020) 174 pp. 26-27.

[29] These are: the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, the initial point of embarkation.

[30] Evaluation of the API Directive, SWD, p. 16. In addition to the data elements listed in the API Directive, as an example, some Member States also request information on the visa, information on other documents used for travel, place of birth, etc.

[31] Evaluation of the API Directive, SWD(2020)174; feedback on inception impact assessment.

[32] For the purposes of the external study supporting this impact assessment, IATA data indicates that 92% of global passengers are offered some kind of self-service check-in option (web, mobile or kiosk), and 57% of global passengers are offered the option to self-board (either by scanning their travel document or through automatic doors). The 2020 evaluation also showed that on routes operated by low-cost carriers, an industry average of 50% passengers do not use check-in desks at the airport. See also External study commissioned by DG Home Affairs, Study supporting an impact assessment: Potential effects of different possible measures on advance passenger information, Final Report, 2021, pp. 83-84.

for collecting API data from passengers. As opposed to manually transcribed information, a more automated collection of the data would lead to less quality issues and a more efficient use of API data, also contributing to the reduction of the time invested by competent national authorities in their interaction with carriers.

2.1.3. How likely is the problem to persist if no action is taken?

Without EU action, the problem will continue to exist and is likely to exacerbate due to the increase of airline traffic and online check-in. This will deepen the fragmentation and discrepancies in the use of API data across Member States. Indeed, if the current rules continue to apply without change, Member States will retain discretion to implement national systems in different manners, leading to different practices as to the use of API data for the pre-checks at the Schengen external borders. This hampers the achievement of the objectives ultimately pursued, that is, improving external border controls.

At the same time, this will also continue to represent a burden on carriers which are confronted with divergent requirements from EU Member States, linked to the lack of harmonisation and limitations in the implementation of the applicable API rules.[33]

2.2. There are security gaps in the processing of air passenger data for law enforcement purposes

2.2.1. What is the problem?

The combined use of API and PNR data is an **effective tool for law enforcement authorities to detect terrorists and other serious criminals**.[34] However, due to the asymmetric material and geographic scopes of API and PNR Directives (see Annex 6), EU law does not ensure that this tool is as effective as it should be, leading to security gaps.

More specifically, API data substantially increases the reliability and effectiveness of PNR data as a tool for the fight against serious crimes and terrorism in the EU. The **joint processing of API data and PNR data** enables the competent national authorities to confirm the identity of passengers. The joint processing of API data and PNR data also informs the competent national authorities whether a passenger has actually travelled and boarded a plane, thereby confirming the travel pattern of suspected individuals.[35]

The use of API data alone would be considered insufficient in the fight against serious crime and terrorism: information on the identity of a passenger without the reservation details (e.g. complete travel itinerary, accompanying passengers, date and modality of ticket reservation

[33] See Evaluation of the API Directive, SWD(2020)174, p. 55; answers to questions 14 and 23 of Study supporting an impact assessment : potential effects of different possible measures on advance passenger information. Annex 7, https://data.europa.eu/doi/10.2837/769718.

[34] See recital 9 of the PNR Directive (Directive (EU) 2016/681): "*Some air carriers retain as part of the PNR data the API data they collect, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that where air carriers collect API data, they transfer it irrespective of whether they retain API data by different technical means as for other PNR data.*".

[35] As confirmed by the 2020 review of the PNR Directive (SWD(2020) 128 final, pp.41-42) and additional targeted consultations with Member State experts for the purpose of this impact assessment (see Annex 2).

or contact details) would not allow establishing or proving links necessary for criminal investigations of serious crime and counter-terrorism cases.[36]

Conversely, based on Member States' operational experience, API data – when collected in an automated way – contains information on the identity of the passenger that is more reliable than PNR data used in isolation.[37] For example, on intra-EU flights where API data is not collected, a comparison of a passenger's PNR data against a database such as the Schengen Information System can generate up to 40 'false-positive' automatic matches due to the absence of personal identifiable information such as the date of birth. This prevents the competent national authorities from making effective use of passenger data for the fight against serious crime and terrorism. Moreover, booking information without reliable information on passenger's identity would not allow competent authorities to determine whether a person has actually travelled, boarded a plane and made use of the booking. API data also helps confirming which booking was effectively used in cases where individuals suspected of serious crimes or terrorism offences made separate bookings (practice of 'broken travel' observed in drug trafficking and counter-terrorism cases).[38]

Consequently, only the joint processing of API data and PNR data enables Passenger Information Units, as set under the PNR Directive[39], to fully 'capitalise' on air passenger data to fight serious crime and terrorism effectively.

Under the current applicable EU legal framework, competent authorities are able to obtain **effective operational results only on flights where both API and PNR data are collected,** namely on extra-EU flights. Competent law enforcement authorities cannot benefit from the results of the joint processing of API data and PNR data for **passengers travelling on flights within the EU for which PNR data is transmitted.[40]** This creates an important **security gap** in the processing of air passenger data.[41] To address this gap, the European Commission's strategy towards a fully functioning and resilient Schengen area of June 2021 identified the collection of API data on intra-EU flights as an additional means to enhance internal security without interfering with travel flows within the EU.[42]

2.2.2. What are the drivers of the problem?

At present, **air carriers do not collect nor transmit API data on flights operating within the EU**. The main driver for this problem is the current legal framework. The API Directive primarily regulates the processing of API data for external border management purposes, and therefore does not address the collection nor the transmission of API data for intra-EU and domestic flights. A collection of API data passengers for border management purposes on

[36] Targeted consultations with national experts (Technical Workshop 2, See Annex 2), confirming the data gathered from surveys sent to national authorities for the preparation of the external *study supporting an impact assessment: Potential effects of different possible measures on advance passenger information.*
[37] European Commission, Staff Working Document accompying the report on the review of the PNR Directive, SWD(2020)128, p.43; Targeted consultations with national experts (See Annex 2).
[38] Targeted stakeholder consultations with Member State experts.
[39] 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
[40] As the regards the collection of PNR data for intra-EU flights, the CJEU has set requirements and safeguards in its ruling in *Ligue des droits humains* case (see below in section 5.2.).
[41] Evaluation of the API Directive, SWD(2020)174, p. 26, 56; Study supporting an impact assessment : potential effects of different possible measures on advance passenger information : final report, https://data.europa.eu/doi/10.2837/014167, p. 39; Targeted stakeholder consultations with Member State experts (Annex 2).
[42] COM(2021) 277 final (2.6.2021).

flights between Member States could amount to an internal border check, contrary to the Schengen Borders Code.

Under the PNR Directive, on flights where API data is also collected by air carriers and therefore available in their systems, API data constitutes an element of the PNR data that air carriers transfer to the Passenger Information Unit.[43] This is, however, only the case for those inbound and outbound flights where Member States request the transfer of API data under the API Directive. Consequently, air carriers do not collect API data for intra-EU and domestic flights and that data is not included in the PNR messages transferred for these flights.

The API Directive does not prevent the **processing of API data for law enforcement purposes** as for provided in national legislation and subject to data protection requirements. However, the implementation of this possibility across Member States is problematic.[44]

- The evaluation of the API Directive showed that the law enforcement purpose is construed widely in national legislation, ranging from administrative offences, enhancing internal security and public order, to fight against terrorism and safeguarding national interests. The API Directive evaluation also indicated that an effective use of API data for law enforcement would require a dedicated legal instrument for this distinct purpose.[45]
- The variety of purposes for collecting API data adds complexity to ensuring compliance with the EU's data protection framework. The requirement to delete API data within 24 hours is established only in the case of the use of API data for the main purpose of the Directive, namely external border management. It is not clear whether this requirement also applies in respect of processing conducted for law enforcement purposes.
- The lack of criteria for the use of API data for law enforcement purposes, namely the API data set that can be requested from carriers for law enforcement purposes, since some Member States (on inbound and outbound flights) currently request API data going beyond the non-exhaustive list included in the API Directive, create additional hindrances for air carriers.
- Likewise, the API Directive gives no indications of the flights for which API data can be requested nor to which authority API data should be transmitted or conditions of access to such data for law enforcement purposes.

The lack of express **EU-wide criteria on the use of API for law enforcement purposes** leads to security gaps.

2.2.3. How likely is the problem to persist?

Without action at EU level, the current situation where the use of the API data for law enforcement purposes is mainly left to national legislation will remain. Diverging practices as to the use of API for those purposes will continue to have an adverse impact on the levels of

[43] Either together with PNR data or separately, if the airline retains API by separate technical means. See Article 8(2) of the PNR Directive: "*In the event that the air carriers have collected any advance passenger information (API) data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the 'push method', those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data*."

[44] Evaluation of the API Directive, SWD(2020)174, pp. 26, 43.

[45] See conclusions of the Evaluation of the API Directive, SWD(2020)174, p. 57.

internal security in the EU, will continue to hinder air industry activities and potentially interfere with passengers' protection of personal data.

This will also continue to create challenges for air carriers having to comply with different obligations across the EU in terms of requirements to transmit API and PNR data. Air carrier associations expressed the wish to see the revision of the API Directive to clarify and harmonise the conditions for the collection of API data for law enforcement purposes.[46]

To compensate for a lack of identity information on passengers on intra-EU and domestic flights, certain Member States introduced so-called "**conformity-checks**" prior to boarding.[47] These entail a visual comparison of the name and surname of the boarding pass against the name and surname of the travel document, at the gate, to ensure that the passenger is the holder of the travel document. Also as a means to offset the increasing use of online check-in on flights operated between Member States, conformity checks were introduced to address the issue of self-declared or 'unverified' nature[48] of PNR data/reservation information and to increase certainty on who is boarding the plane.

Implemented partly as an aviation security measure and partly as a measure to fight terrorism based on national law,[49] conformity checks are an imperfect solution for several reasons. If implemented correctly, such checks only confirm the name and last name of a passenger. They do not allow the confirmation of other identity data (e.g. date of birth, number of travel document, gender). Conformity checks bring significant negative organisational impacts for air carriers, disturbing travel flows at airports where they are implemented (e.g. disturbing automated boarding processes, extension of boarding time, lack of technical solutions to change names at the boarding gate) as well as significant additional costs.[50]

3. WHY SHOULD THE EU ACT?

3.1 Legal basis

As indicated in the 2020 evaluation of the API Directive, the effective use of API data for law enforcement purposes would require a dedicated legal instrument, i.e. an instrument separate from the current API Directive focusing on external border management. Thus, it appears a priori that, for legal reasons, **two separate legal instruments** would be required to regulate the processing of API data for external border management and for law enforcement as two distinct purposes.

For the collection, transmission and use of API data for **border management purposes**, the legal basis would be the same as the one of the current API Directive, namely Articles 77(2)(b) and 79(2)(c) of Treaty on the Functioning of the European Union (TFEU). The instrument on the processing of API data for border management purposes would continue

[46] See feedback received on the inception impact assessment (Annex 2).
[47] In 2020, up to 7 Member States introduced conformity checks on flights between Member States (BG, BE, DK, EE, ES, FR, PT). Source: European Commission, Directorate-General for Migration and Home Affairs, *External Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data*, 2020, pp. 137-140.
[48] As regards the self-declaratory nature of PNR data, see Box 1 (introduction) and Annex 6.
[49] This is for example the case in Belgium and France.
[50] Air France estimated the costs of such a measure up between EUR 2 and 3 million per year. https://www.lefigaro.fr/societes/2018/06/09/20005-20180609ARTFIG00079-air-france-retablit-le-controle-d-identite-des-passagers-a-l-embarquement.php.

to be part of to the Schengen *acquis*. The API data would continue to be processed by the competent border authorities.

For the collection and transmission of API data for **law enforcement purposes**, the legal basis would be the same as the one of the PNR Directive, namely Articles 82(1) (d) and 87(2)(a) of the TFEU. The API data would be transmitted to national authorities (Passenger Information Units) to complement and reinforce the processing of PNR data under the PNR Directive, which is not part of the Schengen *acquis*. Moreover, the collection and further use of API data for law enforcement purposes would be triggered by security needs and not by the crossing of borders as such. Consequently, the separate API legal instrument for law enforcement purposes would not be part of the Schengen *acquis*. The API data would be processed by the Passenger Information Units of these Member States, i.e. the units set up under the PNR Directive, by way of joint processing of API data and PNR data.

3.2. Subsidiarity: Necessity of EU action

The principle of subsidiarity applies since this is an area of shared competence. According to the principle of subsidiarity laid down in Article 5(3) TEU, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

Member States alone would not be able to effectively tackle the problems identified in chapter 2. The need for common rules on the processing of API data for border management is linked to the creation of the Schengen area and the establishment of common rules governing the movement of persons across the Schengen external borders (Schengen Borders Code). In this context, the decisions of one Member State affect other Member States, therefore it is necessary to have common and clear rules and operational practices in this area. Efficient external border controls require a coherent approach across the entire Schengen area, including on pre-checks with API data.

Likewise, Member States alone would not be able to effectively tackle the problems related to the processing of API data for law enforcement purposes. Since the API Directive is a Schengen external border instrument, it cannot regulate the capture and transmission of API data on intra-EU and domestic flights. In absence of API data that would complement the PNR data for these flights, Member States have implemented a variety of different measures that seek to compensate the lack of identity data on the passengers. This includes physical conformity checks to verify identity data between travel document and boarding card (see section 2.2.3) that generate new issues without solving the underlying problem of not having API data.

Action at EU level on API data would therefore be required to address effectively the problems identified in this impact assessment, in accordance with the principle of subsidiarity, as also called for in the June 2021 Commission's *Strategy towards a fully functioning and resilient Schengen area* notably with regard to law enforcement purposes.[51] In addition to the need to reinforce the Schengen area as a political priority of the Union, the need for EU action on API at this point in time also stems from recent legislative developlents on Schengen external border management:

[51] European Commission, Communication to the European Parliament and the Council on '*A strategy towards a fully functioning and resilient Schengen area*', COM(2021)277 final, 2 June 2021, p. 13.

- The 2019 Interoperability Regulation[52] will enable systematic checks of persons crossing the Schengen external borders against all available information in EU centralised information systems for security, border and migration management. Establishing a centralised transmission of API data at EU level is a logical continuation of this concept.
- At the Schengen external borders, the use of API data would effectively complement the imminent implementation of the European Travel Information and Autorisation System (ETIAS) and of the Entry Exit System (EES) (see also annex 7). The use of API data would remain necessary for external border management as it informs border guards in advance whether a traveller has effectively boarded a plane and is about to enter the Schengen area, thus facilitating the border check that will take place once that traveller arrives at the Schengen external border.

3.3. Subsidiarity: Added value of EU action

The Treaty on the Functioning of the European Union (TFEU) explicitly empowers the Union to develop a common policy on the checks to which persons crossing external borders are subject, this is a clear objective to be pursued at EU level. At the same time, this is an area of shared competence between the EU and the Member States.

The 2020 evaluation showed that the API Directive has had a number of positive effects in those Member States that had established a national API system when implementing the Directive and request API data from air carriers.[53] This would not have been realised by Member States acting alone.[54] Using the international standards alone to establish national API systems in the Member States would have been possible without the API Directive but it may not have resulted in a coordinated outcome. However, as indicated in chapter 2, the evaluation of the Directive also showed that the EU legal current framework leads to inconsistent and diverging practices in the Member States on API data requiring further EU action in this area, including with a separate legal instrument on law enforcement.

As illustrated by the effectiveness of existing EU instruments for external border management or law enforcement, such as the Schengen Information System, EU action can bring significant added value to Member States in these areas. Likewise, EU action in response to the problems identified in chapter 2 is expected to address these problems in an effective, efficient and proportionate manner, thereby bringing added value for the management of the Schengen external borders and for internal security in the Union.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

Based on the problem analysis, the general objectives of this initiative are twofold:

1. To enhance Schengen external border management by ensuring that every person crossing the Schengen external border by air undergoes similar and necessary checks prior to entering or leaving the Schengen area.

[52] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa.
[53] The 202 evaluation of the API also showed that Cyprus and Greece did not establish an API system and do not request API data.
[54] Evaluation of the API Directive, SWD(2020)174, p. 51.

2. To enhance the EU's internal security by ensuring that Member States' law enforcement authorities have access to air passenger data that is necessary to prevent and fight terrorism and serious crime.

4.2. Specific objectives

Without overhauling the objectives of the current API Directive in terms of border management[55], the specific policy objectives of the initiative are:

1. **To enhance pre-checks at the Schengen external borders**: Collecting API data at Schengen external borders enables national authorities to cross-check passenger data systematically against information contained in national, EU and international databases, and to do so before a passenger actually arrives at the border crossing point. Receiving API data in advance will introduce efficiencies in the whole process of border checks, providing additional time for analysis of information and thus contributing to the reduction of false-positive matches. It helps border guards to better organise their work at border crossing points, and to better target operations where needed.

2. **To facilitate the flow of bona-fide travellers at the Schengen external borders:** API data facilitates the clearance of low-risk passengers. Better preparation for the control of specific passengers by identifying them via API data in advance of their arrival helps to accelerate border checks as passengers requiring secondary checks can be separated without the other passengers queuing and waiting, thus also reducing waiting times.

3. **To effectively combat serious crime and terrorism with API data complementing PNR data**: API data collected by automated means will uniquely and reliably identify a specific passenger that at some point in time is of particular interest for competent authorities investigating serious crime and terrorism. To allow for the joint processing of API data and PNR data as an effective tool to counter serious crime and terrorism, every PNR data transferred to Passenger Information Units should hence be complemented with complete and correct API data, while respecting the fundamental right to the protection of personal data and the fundamental right to freedom of movement.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

This chapter sets out the available policy options, which include the baseline. The focus is on options requiring a regulatory intervention as the problems identified in this impact assessment are driven by the limitations of the current legal framework. A number of policy options were discarded at an early stage and are described below.

5.1. What is the baseline from which options are assessed?

The baseline is a 'no policy change' scenario.

[55] The current API Directive covers the purposes of improving border controls and combating illegal immigration, and both purposes are covered in this impact assessment by the reference to border management.

With regard to API data collection for pre-checks at the external borders, the baseline scenario would maintain the current legal framework and provisions of the API Directive.

Under the current Directive, air carriers have the obligation to send, upon request of the Member States' authorities, API data on inbound flights crossing the Schengen external borders. Member States have the flexibility to collect API data on a list of selected incoming flights, following a risk-based approach. Therefore, not all Member States collect API data on all inbound extra-Schengen flights. Several Member States have extended the scope of API collection beyond the provisions of the Directive and also collect data for outbound extra-Schengen flights (see section 2.1).[56]

The API Directive contains only a minimum list of data elements that air carriers will have to transmit if requested by competent authorities, and Member States may request additional data other than those mentioned in the Directive. Accordingly, air carriers would continue to be faced with diverging requests and will continue to invest resources to comply with the different individual requirements set by Member States depending on the set up of their national API systems, with multiple transmissions of passenger data to multiple competent national authorities. In turn, national authorities will continue to invest ressources and individual connections with air carriers to effectively receive API data.

Under the current legal framework, Passenger Information Units do not receive API data on selected intra-EU flights.

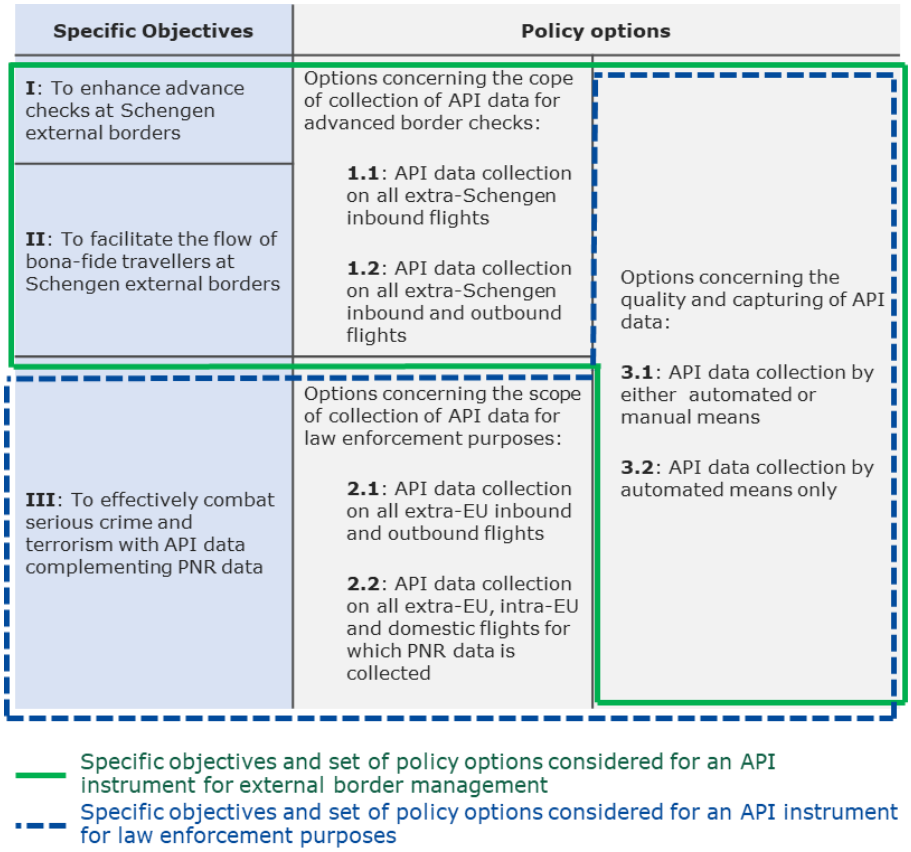
5.2. Description of the policy options

Based on the problem definition and objectives described above, the available policy options can be grouped in three areas of intervention, namely: (1) scope of collection of API data for external border management, (2) scope of collection of API data for law enforcement purposes, and (3) a horizontal aspect on the means to improve the quality of data and the capturing of API that would apply to both purposes, i.e. external border management and law enforcement purposes.

Given the need for two separate legal instruments for the processing of API data for external border management and for law enforcement as two distinct purposes (see section 3.1), the **available options for each envisaged instrument need to be assessed separately**. This is not only because the two separate legal instruments would have different purposes (external border management vs. law enforcement), different legal bases, different national authorities processing the API data (border authorities vs. Passenger Information Units) and different geographical scopes (see above). It is also because the different purposes of border management and law enforcement lead to different assessments in terms of necessity and proportionality of the envisaged intervention. The corresponding policy options are set out in Table 2 below.

Table 2: Overview of policy options against specific objectives pursued by the initiative

[56] Data gathered from surveys sent to national authorities for the preparation of the external study supporting an impact assessment: Potential effects of different possible measures on advance passenger information, see annex 7.



In addition, the initiative would have the following components that are technical and non-controversial in nature and therefore not assessed in this impact assessment:

- As regards the types of flights, the initiative would cover all commercial flights, scheduled and non-scheduled (including charter flights and business aviation).
- The collection of data would involve all passengers and crew members, regardless of their nationality.
- A full set of API data would include identity information as contained in the travel document, as well as flight information, and seating and luggage information (see Annex 5).
- API data would be transmitted through one single entry point at EU level (the carrier interface, see Annex 7).

5.2.1. Options concerning the scope of collection of API data for Schengen external border management

There are two policy options for extending the scope of API data to enhance the management of the Schengen external borders:

Policy option 1.1*: API data collection on all extra-Schengen inbound flights*

This policy option provides for the **systematic** collection of API data on all extra-Schengen **inbound flights** for the purpose of Schengen external border management. This means there will be no prioritisation of flights or collecting API data on selected flights under this policy option.

This policy option sets an **obligation on Member States** applying the Schengen *acquis* and on Schengen Associated Countries to collect and request API data on all flights coming from outside the Schengen area, in contrast to the current situation where the collection of API data is subject to risk and operational assessments by national authorities. Competent border authorities will use API data for pre-checks against the databases set out in the Schengen Borders Code.[57]

Therefore, under this policy option, **air carriers would be obliged to collect and transmit API data for all extra-Schengen inbound flights**.

As the current 24-hour retention period of the data is too short for competent border authorities to carry out pre-checks effectively (e.g. due to long haul flights), this policy option would provide for the retention of API data by competent border authorities for 48h.[58] Such retention would be proportionate because the data would not be retained for longer than what is necessary to carry out pre-checks.

The processing of API data by air carriers and competent national authorities under this policy option would have to comply with the **General Data Protection Regulation**.[59]

Policy option 1.2*: API data collection on all extra-Schengen inbound and outbound flights*

This policy option provides for the **systematic** collection of API data on all extra-Schengen **inbound and outbound flights** for the purpose of external border management. There would be no prioritisation of flights, or API data collection on selected flights, under this policy option.

The API Directive neither requires nor excludes the possibility to collect API data on outbound flights. Some Member States already request API data on such flights for law enforcement purposes.[60] Moreover, API data is collected by air carriers on certain outbound flights as such flights qualify as inbound flights for third countries requesting API data.

Therefore, under this policy option, **air carriers would be obliged to collect and transmit API data for all extra-Schengen inbound and outbound flights**. The API data of all air passengers entering and leaving the Schengen area would be transmitted to competent border authorities for their processing.

This policy option would therefore set a new **obligation to Member States** applying the Schengen acquis and on Schengen Associated Countries to collect and request API data on all flights entering and leaving the Schengen area. Competent border authorities would receive this data to check air passengers against those databases referred to in the Schengen Borders Code.

---

[57] Article 8 of the Schengen Borders Code (Regulation (EU) 2016/399). The Schengen Borders Code provides that border checks on persons should include the verification of the identity and the nationality of the person and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular the Schengen Information System, Interpol's Stolen and Lost Travel Documents (SLTD) database and national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

[58] Evaluation of the API Directive, SWD(2020)174, p. 57; confirmed by targeted stakeholder consultations with Member State experts (Annex 2).

[59] 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

[60] This was the case for Belgium, Bulgaria, Denmark, Estonia, Finland, France, Lithuania, Poland, Romania, Slovenia and Slovakia, as found in the Evaluation of the API Directive, SWD(2020)174, p. 15.

The processing of API data air carriers and competent national authorities under this policy option would have to comply with the **General Data Protection Regulation**.[61]

5.2.2. Options concerning the scope of collection of API data for law enforcement purposes

The policy options set out in this section address the collection and transmission of API data for law enforcement purposes to allow for the joint processing of API data and PNR data. Consequently, these policy options align the purposes of API data collection to the purposes of the PNR Directive, namely to **detect, investigate and prosecute terrorist offences –** as defined in the Directive on combating terrorism[62] **and serious crime** – as listed in Annex I of the PNR Directive. For these policy options, 'law enforcement purposes' refers to the prevention, detection, investigation and prosecution of terrorist offences and serious crimes.

The scope of the policy options set out in this section is limited to regulating the **collection** of API data by air carriers and the subsequent **transmission** of the API data to competent authorities, namely the Member States' Passenger Information Units (PIUs) set up under the PNR Directive. The Passenger Information Units that would receive and process the API data by way of joint processing of API data and PNR data in accordance wih the PNR Directive which already provides the Passenger Information Units with a legal basis to process API data they receive.[63]

The applicable **rules on API data processing** for the detection, investigation and prosecution of terrorist offences and serious crime, as well as the safeguards for the protection of fundamental rights, in particular the right the protection of personal data, **would be those provided by the PNR Directive**. Importantly, this would include the requirements and safeguards for the processing of data that the Court of Justice of the EU (CJEU) articulated in the ***Ligue des droits humains*** **case** in the light of the Charter of Fundamental Rights of the EU ('the Charter').[64] Given the close interrelationship between PNR data and API data and the fact that the Court's interpretation was mostly based on the Charter, the policy options set out in this section would be subject to the requirements articulated in this ruling.

Given the sensitivities around the processing of API data for **all extra-EU, intra-EU and domestic flights**, this will be assessed in a dedicated policy option 2.2.

Policy option 2.1*: API data collection on all extra-EU inbound and outbound flights*

This policy option provides for the **systematic** collection of API data on all extra-EU **inbound and outbound flights** for law enforcement purposes.

This policy option sets an **obligation on Member States** to request and collect API data on all flights entering or leaving the EU. There would be no prioritisation of flights under this policy option.

---

[61] 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

[62] Directive (EU) 2017/541 of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

[63] See Article 8(2) and Annex II of the of the PNR Directive.

[64] CJEU, iudgment of 21 June 2022, case C-817/19, Ligue des droits humains.

Therefore, under this policy option, **air carriers would be obliged to collect API data for all extra-EU inbound and outbound flights** and transmit it to the Passenger Information Units of the Member States concerned. Consequently, the API data of all air passengers entering or leaving the EU would be processed under this policy option.

This policy option would ensure that API data is available to Passenger Information Units for the joint processing of API data and PNR data for all flights entering or leaving the EU, supporting them in their risk analysis of all travellers entering and leaving the EU. The collection of API data for law enforcement purposes under this policy option would be **triggered by security needs** – as reflected in the PNR Directire that requires the collection of PNR data for all extra-EU inbound and outbound flights – and not by the crossing of external borders. Consequently, for law enforcement purposes, extra-EU inbound and outbound flights can be assessed under one policy option.

The processing of API data by air carriers under this policy option would have to comply with the **General Data Protection Regulation** Under this policy option, the subsequent processing of API data by the Passenger Information Units takes place under the requirements and safeguards set by the **PNR Directive**, as interpreted by the CJEU in the ***Ligue des droits humains* case**. Under this policy option, any subsequent processing of the data by national law enforcement authorities (other than the Passenger Information Units) would have to comply with the conditions for processing set in the PNR Directive[65] and also with the the **Law Enforcement Directive**.[66]

Policy option 2.2*: API data collection on all extra-EU inbound and outbound flights, intra-EU and domestic flights for which PNR data is collected*

This policy option provides for the collection of API data on **all extra-EU flights, both inbound and outbound flights, and on selected intra-EU and domestic flights** for law enforcement purposes, namely on those flights for which PNR data is collected under the PNR Directive.

This policy option sets an **obligation on Member States** to request and collect API data on all extra-EU, intra-EU and domestic flights on which they collect PNR data. Consequently, when they select intra-EU and domestic flights for which they request air carriers to transmit PNR data, there would be a selection of flights under this policy option following the threat assessment that Member States have to carry out , in accordance with the requirements and safeguards of the PNR Directive in this regard, as interpreted by by the CJEU in the *Ligue des droits humains* case in the light of the Charter.

Therefore, under this policy option, **air carriers would be obliged to collect API data for all extra-EU flights, intra-EU and domestic flights for which they transmit PNR data,** and transmit that API data to the Passenger Information Units of the Member States concerned. Consequently, only the API data of air passengers on these selected flights intra-EU and domestic flights would be processed.

[65] Article 7 of the PNR Directive.

[66] Directive (EU) 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.

This policy option would ensure that API data is available to Passenger Information Units for the joint processing of API data and PNR data for all extra-EU, intra-EU and domestic flights for which Member States already collect PNR data in accordance with their risk assessments. More specifically, the collection of API data on intra-EU and domestic flights would be **triggered by security needs**, i.e. the same security needs that made Member States apply the option of PNR data processing for intra-EU and domestic flights under the PNR Directive.

It should be clear that the collection of API data under this policy option would not be triggered by the crossing of internal borders in the absence of internal border checks, since it would apply both to selected intra-EU and domestic flights. The policy option would be consistent with the December 2021 **proposal to revise the Schengen Borders Code**[67] which clarifies that the Schengen Borders Code would not prevent the use of passenger data such as API data for pre-checks against databases on passengers for security purposes on connections between Member States in case this would be allowed by applicable law.

The processing of API data on intra-EU and domestic flights by air carriers under this policy option would have to comply with the **General Data Protection Regulation**.[68] Under this policy option, the subsequent processing of API data by the Passenger Information Units takes place under the requirements and safeguards set by the **PNR Directive**, as interpreted by the CJEU in the ***Ligue des droits humains* case**, notably what is specified in that case regarding the processing of PNR data for intra-EU flights (see box 2 below). Under this policy option, any subsequent processing of the data by national law enforcement authorities would have to comply with the conditions for processing set in the PNR Directive[69] and also with the the **Law Enforcement Directive**.[70]

Box 2: The collection of PNR data on (all or selected) intra-EU flights

In the recent *Ligue des droits humains* case, the the CJEU considered that the (possible) collection of PNR data on intra-EU flights by Member States should not go beyond what is strictly necessary[71]:

- PNR data collection on **all intra-EU flights** is only possible where a Member State establishes that there are **sufficiently solid grounds for considering that it is confronted with a genuine and present or foreseeable terrorist threat**. Such collection should be limited in time and the decision taken by a Member State to collect PNR data on all flights must be open to effective review (by a court or by an independent administrative body).

- **in the absence of a genuine and present or foreseeable terrorist threat**, Member States may not collect PNR data on all intra-EU flights. In such cases, PNR data collection PNR data collection for those flights is possible on **selected intra-EU flights** relating, for example, to certain routes or travel patterns or to certain airports for which there are, according to the assessment of the Member State concerned, indications that would justify that application. Data collection on selected intra-EU

[67] See amendments to Article 23(e) in the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders, COM(2021) 891 final, 14.12.2021.
[68] 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
[69] PNR Directive sets conditions for the procession of the data such as the competent authorities involved (Article 7), period of data retention (Article 12) and protection of personal data (Article 13).
[70] Directive (EU) 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.
[71] CJEU, iudgment in case Case C-817/19, *Ligue des droits humains*, paras. 171-174.

flights should also be regularly reviewed by the Member State in accordance with changes in the circumstances that justified their selection.

5.2.3. Options concerning the quality and capture of API data

The policy options sets out in this section provide horizontal means to improve the quality and capturing of API data that would apply to the collection of API data on any applicable flight and for any purpose, thus affecting both the collection of API data for Schengen external border management and and the collection of such data for law enforcement purposes.

A first step to improving the quality of API data is to make it compulsory for air carriers to collect the same **complete set** of API data elements. This initiative would therefore introduce a closed list of API data, mandatory on all flights where API data is requested. This is to align the API data elements to the identity data found in the Machine Readable Zone (MRZ) of a passport, the default travel document, or an identity card (see box 3).

Box 3 : Machine Readable Zone (MRZ)

The MRZ is an ICAO standard[72] that enables cameras to take a picture of these 'precise black' characters and transform them into a digital format, a process known as Optical Character Recognition (OCR). When successfully using OCR, the data is correct and complete.

EU rules for the issuance of passports and travel documents by Member States provide that these documents must contain a machine-readable biographic information, in compliance with ICAO standards.[73] In addition, the Regulation on the strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members provides that identity cards issued as of 2023 shall also contain a machine readable zone on national identity cards issued to EU citizens.[74]

Policy option 3.1*: API data collection by either automated and manual means*

This policy option provides for measures to improve the quality of API data by clarifying by which methods API data would be captured. This would entail the capture of API data from the MRZ through automated means, such as devices using technologies (e.g. OCR). Where other travel documents have been used, such as national identity cards, collection of API data could also be considered, provided they have an MRZ as per ICAO standards.

This policy option therefore foresees a range of methods to capture API data:

[72] https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf; see also Annex 5.
[73] Council Regulation (EU) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States
[74] Regulation (EU) 2019/1157 of the European Parliament and of the Council on on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement

- **Scanning the MRZ**: For passengers agreeing to do so, online check-in would imply passengers using electronic devices to scan the MRZ of their travel document. More specifically, the passenger would use a secure app on a smartphone or webcam to take (a) picture(s) of the travel document during the on-line check-in process. The carrier's IT-systems would perform the OCR and transmit complete and correct identity data as part of API message.
- **Provision of API data at the airport**: For those passengers not wanting or not being able to use the above method during on-line check-in, the travel document's MRZ would be read by a member of staff by automated means during check-in or boarding at the airport, or by automated means at a self-service kiosk at the airport, without any additional fees for such service.
- **Online or web-check-in**: Those passengers not wanting or not being able to use the above-mentioned methods would still be able to enter manually their data.

Consequently, this policy option provides for the establishment of clearer definition of data quality thresholds, which, if detected and unmet, would result in **financial sanctions for the air carriers**. Each of these different methods would imply different levels of carrier liability and therefore different levels of sanctions. For instance, the level of data accuracy and completeness is higher where data is collected by automated means involving a scan of the travel document's MRZ,[75] therefore resulting in less missing data fields or errors inducive of sanctions.

Policy option 3.2*: API data collection by automated means only*

Compared to the previous policy option, this policy options provides for mandating automated collection of API data only:

- **Scanning the MRZ**: For passengers agreeing to do so, online check-in would imply passengers using electronic devices to scan the MRZ of their travel document. More specifically, the passenger would use a secure app on a smartphone or webcam to take (a) picture(s) of the travel document during the on-line check-in process. The carrier's IT-systems would perform the OCR and transmit complete and correct identity data as part of API message.
- **Traditional check-in at the airport**: For those passengers not wanting or not being able to use the above method during on-line check-in, the travel document's MRZ would be read by a member of staff by automated means during check-in or boarding at the airport, or by automated means at a self-service kiosk at the airport, without any additional fees for such service.

The possibilities of manual entry at check-in and online manual self-declaration of API data by the passenger would be eliminated. Traditional assisted airport check-in would still be possible for passengers not wanting or not able to use electronic devices to scan the MRZ. Air carrier staff performing the check-in at the counter would have to be equipped with MRZ scanners or other solutions to ensure the automated collection of the MRZ.

[75] MRZ detection or character reading accuracy from dedicated scanners at check-in kiosks and counters is close to or at 100%. See, for instance: Liu, Y., James, H., Gupta, O. and Raviv, D., *MRZ code extraction from visa and passport documents using convolutional neural networks*; Association for the Advancement of Artificial Intelligence, 2020, available at: https://arxiv.org/pdf/2009.05489.pdf; Hartle, A, Arth, C, and Schmalsteig, D., Real-time Detection and Recognition of Machine-Readable Zones with Mobile Devices, 2015, available at: https://www.scitepress.org/Papers/2015/52947/pdf/index.html.

This policy option would mean that no fines could be imposed by national authorities on air carriers for errors in the collection of API data. Where air carriers collect API data exclusively by automated means, there are no possibilities of errors in that collection.

5.3.Policy options discarded at an early stage

Following the stakeholder consultations and the activities carried out in preparation of this impact assessment (Annex 2), the following options were discarded.

5.3.1. API data collected on transit flights for advanced border checks

As opposed to direct flights, transit (or connecting) flights enable passengers to reach the final destination through two or more flights, after a brief stop-over at the airport. One single ticket is issued and the passenger does not change planes or airlines. In such cases, the advance passenger data is sent by the air carrier to the final destination country that will effectively perform the entry border check of passengers.

For example, a flight from New York to Ankara with a stop in Frankfurt, will not lead to API data being delivered to Germany. The passenger would not enter the Schengen area in Frankfurt and would not undergo an entry check at the external borders.

5.3.2. API data transmitted for law enforcement purposes on all intra-EU flights

This option would create a new obligation on Member States to systematically request API data on **all** intra-EU flights for law enforcement purposes, including on flights where PNR data would not be processed by Member States. On those flights where no PNR data is processed, the added value of processing API data alone for law enforcement purposes would be limited (see also section 2.2). In addition, considering the requirements and safeguards articulated in the recent in the *Ligue des droits humains* case,[76] the transfer of API data on all intra-EU flights would be a serious interference with passengers' fundamental right to the **protection of personal** data (Article 8 of the Charter) that would only be justified in the situation of a genuine and present or foreseeable terrorist threat. In the absence of such a threat, the transfer of API data on all intra-EU flights would therefore not meet the necessity and proportionality requirements. Moreover, the Court also provided guidance on the fact that the collection of PNR data linked to cross-border travel within the EU could deter the exercise of the fundamental right to **freedom of movement** (Article 45 of the Charter) and therefore constitute a restriction of that freedom.[77] Considering this guidance, the transfer of API data on all intra-EU flights would not be compliant with the freedom of movement.

While the idea of transmitting API data on all intra-EU flights was discussed with stakeholders during consultations, this policy option must be discarded following this ruling.

5.3.3. API data collected from other means of transport (maritime, rail, bus)

The Schengen Borders Code provides that, as regards **maritime operators**, crew and passenger information must be transmitted by maritime carriers to border authorities as a list

[76] CJEU, iudgment of 21 June 2022, case C-817/19, *Ligue des droits humains*, paragraphs 171-174. See also box 2 above.
[77] CJEU, iudgment of 21 June 2022, case C-817/19, *Ligue des droits humains*, paragraphs 278-279.

containing the information required in the FAL form 5 (crew list) and FAL form 6 (passenger list) of the Convention on Facilitation of International Maritime Traffic (FAL Convention), as well as visa or residence permit numbers, where applicable.[78] These data must be transmitted at least 24 hours prior to the scheduled arrival of the vessel.

Therefore, EU and international obligations already exist on maritime transport operators to collect and transmit in passenger information in advance to border authorities of Member States on incoming and outgoing routes. In this context, any additional requirement to transmit 'API' data in a separate instrument, would be redundant and create considerable burden on maritime operators.

Contrary to air and maritime transport sectors, there are no international standards nor EU obligations for the collection of passenger data from land transport operators such as **rail or bus**. Rail transport has specific characteristics in terms of infrastructure, passenger journey and density of networks. Such observations can also be extended to the bus transport sector, composed of a variety of small to medium sized companies. Compared to the air transport sector, the collection of passenger data is more challenging as the issuing of nominative tickets is not a standard practice. To introduce a systematic collection and use of API data for rail and/or bus transport would require heavy investments in the physical infrastructure of operators, with substantial consequences on their economic model and on passengers.

At national level, some Member States have implemented, based on national law, requirements to collect passenger data on rail connections with third countries.[79] Such national practices will not be affected by this initiative.

5.3.4. API data collected for contact tracing[80] for health purposes

The recent COVID-19 pandemic led to reflecting how passenger data could support the protection of public health and prevent the spread of infectious diseases. During stakeholder consultations carried out for this impact assessment (see Annex 2), the Commission services explored opportunities to expedite the cross-border contact tracing of passengers[81] and therefore create synergies with other instruments under which air carriers communicate passenger data to national authorities, including API and PNR Directives.

For contact tracing purposes, information from passengers including contact details such as phone number(s), email address, or a physical address are the relevant data elements that are required to ensure necessary follow-up actions by the authorities. Among the collection of passenger data regulated at EU level, PNR data contain information that may help tracing routes of passengers coming from risk areas and track passengers that have been sitting in the proximity of infected passengers thanks to the availability of seat and other contact information in the PNR data set. However, the PNR Directive currently allows the processing of PNR data only for the fight against terrorism and serious crime, with no

[78] As per Annex VI Chapter 3 of the Schengen Borders Code (Regulation 2016/399/EU).
[79] e.g. Estonia and Finland on the high speed train connections with Russia.
[80] Contact tracing is the identification and information of people who may have been exposed to a source of infection through contact with an identified sick person in order to ensure that they take the necessary measures to prevent the spread of the disease (source: https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19).
[81] European Commission, Proposal for a Regulation on serious cross-border threats to health and repealing Decision No 1082/2013/EU, COM(2020)727 final.

exceptions, as confirmed by the recent judgment of the CJEU in the *Ligue des droits humains*.[82]

As a tool allowing to identify passengers, API data will not contain contact details of passengers. A possible future revised PNR instrument could conceivably contribute to contact tracing to the extent that this is seen as operationally justified and legally and technically possible. That would have to be assessed separately.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This chapter assesses the impact of the policy options identified in section 5.2 against a series of categories, in line with the Better Regulation Guidelines.

The baseline scenario is unsuited to address the problems identified in chapter 2, and will therefore not be further assessed.[83]

The **social impacts** assessed in this chapter focus on implications for the security for both the EU and travellers and on impacts on travel facilitation. Where applicable, and in addition to the specific assessment of the impact on the fundamental right to freedom of movement (see below), the section on social impacts will include an assessment of the practical implications of the collection of API for intra-EU and domestic flights on the exercise of free movement and compliance with the free movement acquis.

The **economic impacts** of the policy options assessed in this chapter will concern impacts on national authorities and air carriers. The selected impacts are assessed quantitatively and qualitatively based on a number of key assumptions (see annexes 3 and 4). The costs will fall to the EU budget and Member State authorities operating the systems. The proposed measures are not expected to have a significant impact on small and medium sized enterprises.

This chapter also assesses the policy options in terms of their **impact on the exercise of fundamental rights** protected by the Charter, with a focus on the **right to the protection of personal data** as guaranteed by Article 8 of the Charter. This chapter also addresses other fundamental rights enshrined in the Charter, namely the right to **freedom of movement** (Article 45), the **freedom to conduct a business** (Article 16), the right to an **effective remedy** (Article 47) and **non-discrimination** (Article 21).

No significant **environmental impacts** are expected from this initiative. The initiative is not expected to have an impact on the volume of air travel. The identified policy options will as such not affect the emissions of greenhouse gases in the atmosphere by air transport operators, or the anticipated demand for air passenger transportation.

6.1. Social impacts

The social impacts of the initiative are twofold: (a) there are important (positive) implications for external border management and hence for security in the EU at large, and

[82] CJEU, iudgment in case Case C-817/19, *Ligue des droits humains*, 21 June 2022, ECLI:EU:C:2022:491.
[83] For more information on the effectiveness and efficiency of the implementation of the current API Directive, please see the evaluation of the API Directive completed in 2020 (SWD(2020) 174).

(b) there is an impact on the speed and convenience of travelling and more broadly on air travel facilitation.

Policy option 1.1 – *API data collection for border management purposes on all extra-Schengen inbound flights*

This option would ensure that all travellers are pre-checked in a consistent way upon arrival at external borders. This would positively impact external border management and hence security in the EU at large, as it permits the identification of passengers who would not be allowed to enter the territory of a Member State and/or using false travel documents. Complementing the implementation of the European Travel Information and Authorisation System and of the Entry Exit system, where air carriers need to determine whether a third country national holds the necessary authorisations to enter the Schengen area (see section 3.2), API data is the tool which informs border guards in advance whether a traveller, regardless of its nationality, is about to arrive at the Schengen external border by air travel. It provides competent border authorities with a tool to effectively and efficiently cross-check all passengers by organising in advance their border control activities, thus facilitating and accelerating the entry of all passengers to the Schengen area.

Policy option 1.2 – *API data collection for border management purposes on all extra-Schengen inbound and outbound flights*

This option would ensure that all travellers are pre-checked in a consistent way upon arrival and upon departure from the Schengen area. Collecting API data on passengers entering and leaving the Schengen area would have a limited impact on external border management. More specifically, collecting API data on passengers leaving the Schengen area would not have an impact on external border management as these passengers would have passed the Schengen external border check at the moment of transmission of API data. Consequently, the impact on travel facilitation would be neutral (the positive effects of the entry of passengers on inbound flights counterbalanced by the limited facilitation of passengers of this policy option on outbound flights).

Policy option 2.1 - *API data collection for law enforcement purposes on all extra-EU inbound and outbound flights*

This option would have a strong positive impact on the robustness of the EU internal security architecture. Making high quality, verified API data systematically available to Passenger Information Units on all extra-EU inbound and outbound flights would boost the effectiveness of their PNR processing and enhance considerably the fight against serious crime and terrorism. The joint processing of API data and PNR data would provide a tool for law enforcement authorities to track the movements of known suspects and to identify suspicious travel patterns of unknown individuals who may be involved in criminal and terrorist activities. This would close an important gap in the use of passenger data for law enforcement purposes and complement the PNR Directive.

In terms of passengers' convenience and travel facilitation the impact of this option is neutral.

Policy option 2.2 - *API data collection for law enforcement purposes on all extra-EU flights, intra-EU and domestic flights for which PNR data is collected*

By closing a gap on intra-EU and domestic flights where the absence of API data undermines the reliability of PNR data processing in the fight against serious crime and terrorism, this option would represent an important contribution to the EU's internal security. It would again boost the quality and effectiveness of PNR processing (up to the extent that this is applied by Member States for intra-EU and domestic flights), much more effectively than the implementation of 'conformity checks' by individual Member States (see section 2.2.3). As no consistent security checks on intra-EU and domestic flights are being performed today due to the absence of API data on those flights, this option would address a very important security gap, and would have a very significant positive impact on internal security. Notably, it would allow for the combined processing of API and PNR data on selected intra-EU and domestic flights as an effective tool to counter serious crime and terrorism, providing a tool for law enforcement authorities to track the movements of known suspects and to identify suspicious travel patterns of unknown individuals who may be involved in serious criminal and terrorist activities when they travel within the EU. This would close an important security gap in the use of passenger data for law enforcement purposes and complement the PNR Directive which allows Member States to collect PNR data on selected intra-EU and domestic flights.

As API data is currently not collected for intra-EU and domestic flights, this option would have an impact on travel convenience and facilitation. This impact is however limited. The (self-) capturing of API data is an integrated component of the check-in process, which takes very little effort and time, especially when supported by automated means (see policy options 3.1 and 3.2). In that respect, the practicalitites of the (self) capturing of API data must be designed in a way that mitigates any risk of a chilling effect on the freedom of movement.[84] To that end, passengers not willing or able to scan their travel document electronically must have the possibility to provide their API data at a check-in desk, a self-service kiosk or during boarding at the airport see option 3.2 below).

Policy option 3.1 - *API data collection by either automated or manual means*

As regards impacts on security, this option represents a potential improvement as compared to the baseline scenario. Manual entry of data from travel documents during online check-in would continue to be possible, leading to a continued probability of mistakes being made.

In terms of passengers' convenience and travel facilitation, this option provides travellers with a full range of solutions to accommodate different levels of digital literacy, allowing them to collect information contained in their travel document in various ways.

Policy option 3.2 - *API data collection by automated means only*

This option would have a clear positive impact on security, as the collection of API data through automated means only would significantly increase the accuracy and completeness of data received by the authorities.

[84] See the Fundamental Rights Agency's submission to the CJEU in Case C-817/19, paras. 60-69; and Fundamental Rights Agency (2014), Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data, para. 7.

Under this option travellers would no longer be able to manually insert their API information during online or web-check-in. This would however be mitigated (for those passengers not willing or able to scan their travel document electronically) by the possibility to provide their API data at a check-in desk, a self-service kiosk or during boarding at the airport, hence mitigating any risk of a chilling effect on the freedom of movement.

6.2. Economic impacts

When assessing the economic impacts of the initiative a distinction is to be made between (1) the impact on Member States, and (2) the impacts on air carriers. Assumptions and calculations underpinning the assessment presented in this section are presented in more detail in Annex 4.

Policy option 1.1 – *API data collection for border management purposes on all extra-Schengen inbound flights*

The economic impact of this option on competent authorities in **Member States** applying the Schengen *acquis* and the Schengen Associated Countries would depend on the number of routes that national API systems already cover. This situation varies greatly between Member States. Also, the size of a Member State, the number of airports and the overall volume of inbound flights would influence the costs of this option for a specific Member State. Either way, national API systems would need to be modified to receive and process additional data flows that were not previously collected, such as passenger data from charter and business flights. A quantification of these additional costs and upgrades of existing systems is very difficult (Member States were unable to provide estimates when requested). Based on available estimates for setting up national API systems, the costs for necessary adaptations to deal with an increased volume of API data for inbound flights can however be estimated at an average EUR 0,5 million per Member State, or **EUR 13,5 million** in total.

As for the costs for **air carriers**, the starting point is that commercial air carriers transporting passengers to the EU are already requested to send API data on most flights. Most large commercial airlines already have the capacity to collect such data via automated means, systems or applications. In contrast, those operating non-scheduled flights (charter flights and business aviation) may not be equipped with IT systems to systematically collect API data. However, solutions such as collecting and transmitting API data via web applications are currently being used and made available by national authorities.

As explained in Annex 4, one of the main cost elements for air carriers lies in the transmission costs of API data. An obligation to transmit API data systematically on all inbound flights represents an increase in the volume of data transmitted and therefore result in additional costs of transmission of API data. At present, air carriers can be requested to transmit API data twice: to competent border authorities and to Passenger Information Units. With this initiative API data would be transmitted to a single point, namely the carrier interface accompanied by an API router, which would substantially reduce the transmission costs for air carriers.

Accordingly, the net additional annual API transmission costs for air carriers on inbound flights for border management purposes would in future be **lower** than today. Whereas currently API data is transmitted for around 65% of inbound travellers, *twice*, under this initiative this would be done for 100% of passengers, but only *once*. This results in a net saving for the airline industry of **EUR 2,53 million** per year.

Policy option 1.2 – *API data collection for border management purposes on all extra-Schengen inbound and outbound flights*

Like for option 1.1, the economic impact on competent authorities in **Member States** applying the Schengen *acquis* and the Schengen Associated Countries would depend on the number of routes that national API systems already cover, and therefore the overall volume of outbound flights from the country concerned in addition to the inbound flights. Most Member States do not yet collect API data on outbound flights (see Chart 1).

Building on similar estimates as used for option 1.1, the costs for necessary adaptations by Member States for collecting and processing API data on outbound flights would be an average of EUR 2 million per Member State, or EUR 54 million in total. These costs would add up to the estimates for collecting an processing API Data on inbound flights, therefore the total costs for Member States' authorities would amount to a total of **EUR 67.5 million**.

Regarding the economic costs of this option for **air carriers**, it must be born in mind that the EU's outbound flights are inbound flights for third countries, for which API is already being collected, or will be collected soon, in line with international obligations. In practice, the burden for *acquiring* API data for these flights is therefore already present for air carriers and is not different than for acquiring API data on inbound flights.

As for the actual *transmission* of this data to competent border authorities and to Passenger Information Units on both inbound and outbound flights , this initiative would incur costs on air carriers. As under option 1.1, this would be partly offset by the introduction of the carrier interface accompanied by an API router. The net actual transmission costs for air carriers on inbound and outbound flights for border management purposes is estimated at **EUR 1.68 million** per year.

Policy option 2.1 - *API data collection for law enforcement purposes on all extra-EU inbound and outbound flights*

The national authorities set to use API data for law enforcement purposes on all extra-EU flights are the **Passenger Information Units**, which are established in all Member States. These authorities already receive and process API data as a PNR complement on all flights for which such data is being collected under national legislation. The proposed initiative measures would increase the volume of API data processed, but as this is part and parcel of PNR data processing the associated costs cannot be calculated. However, as the API data-set is smaller than the PNR data-set currently processed by PIUs on extra-EU and intra-EU flights, the assumption is that PIUs would incur only a negligible amount of additional costs.

This option would only produce an net cost of **EUR 4,21 million** for **air carriers** in the case that 1.1 is retained. In the case option 1.2 is chosen as API data would have been already collected and transmitted for border management purposes on inbound and outbound flights no cost is incurred.

Policy option 2.2 - *API data collection for law enforcement purposes on all extra-EU, intra-EU and domestic flights for which PNR data is collected*

Like under option 2.1, the recipients of API data collected on all extra-EU (both inbound and outbound flights) and on intra-EU flights would be the Member States' **Passenger Information Units** (PIUs). As API data is not being collected today on selected flights

within the EU, the proposed initiative would effectively lead to an increase of the amount of API data that would be received and would need to be processed. However, as this processing is again part of PNR data and the associated cost for this increased data handling would therefore be very small, if not negligible.

Commercial airlines do not currently collect nor transmit API data on intra-EU flights. This means that under this option **air carriers** may need to bring changes to their IT systems in order to be able to do so. This applies notably to the air carriers that exclusively operate within the EU. The corresponding total costs for the industry are estimated at **EUR 75 million**. In case it would be decided by airlines to pass these costs on passengers, this would correspond to a price increase of 5 cents of the plane ticket, if spread over a period over three years.

In addition to these one-off investment costs, this option would also involve transmission costs for air carriers. Net transmission costs of information exclusively transmitted for law enforcement purposes for all extra and intra EU as well as for domestic flights depend on the option chosen for border management purposes. They are estimated at EUR 20,35 million per year in case option 1.1 is chosen (EUR 16.14 million recurrent costs for the transmission of API data on intra-EU and domestic flights and EUR 4.21 million recurrent costs on outbound flights), and at EUR 16,13 million in case option 1.2 is chosen.[85] If airlines would shift this transmission cost to consumers it would increase the ticket price by 1,8 cents (see annex 3).

Policy option 3.1 - *API data collection by either automated or manual means*

Under this option, national authorities of **Member States** – both border management authorities and PIUs – would benefit from the improved API data quality and harmonisation of data sets: more accurate data would lead to more efficient processes and cross-checks against other databases. The economic impact can therefore be rated as positive, albeit it is impossible to quantify this in financial terms.

As regards the impact on **airlines**, they could – under this option – chose to bring modifications to their online check-in systems if they wish to collect API data using automated means. Under this policy option, they would however still be subjected to fines in case of erroneous transmissions. The total amount of potential sanctions incurred by air carriers in the EU is estimated at up to EUR 80 million per year.

Policy option 3.2 - *API data collection by automated means only*

As explained in the section on social impacts, this option is expected to cater for an even higher level of data quality than option 3.1. As the probability of errors in the transmission of API data would be significantly reduced, **Member States**' authorities would likely need less (human) resources to check the quality of the data and save time in engaging with air carriers for fines. The again justifies a positive (and actually higher) economic rating, without however being able to quantify this.

[85]The net transmission costs of the outbound flights shall not be counted twice, i.e. once for the purpose of border management, and a second time for law enforcement purposes. Therefore, net transmission costs for API data for law enforcement purposes do not take into account those already covered for the purpose of border management, and hence depend on the policy option which was chosen for border management. If policy option 1.2 was chosen over 1.1, the transmission costs for border management would cover API for outbound flights, and hence, should not be counted for law enforcement. Conversely, if policy option 1.1 was chosen, costs for outbound flights would not count for border management but will have to be covered by option 2.2 for law enforcement purposes.

Under this option **airlines** would be obliged to make available online check-in systems and collect API data, using automated means only. Many airlines have already put such systems and functionalities in place, yet further investments may still be needed to further roll out this approach throughout the organisation. Other airlines may still need to make modifications and adaptions to their systems. Whereas the costs of the required efforts may therefore be unevenly distributed between airlines, it is estimated that the required one-off costs for the industry as a whole is in the range of **EUR 50 million**.

Collecting API data with automated means only also generates important savings for the airline industry. It would increase the efficiency of their passenger handling workflow, thereby reducing the accompanying costs. It would also reduce the risk for air carriers to be exposed to sanctions for non-compliance and transmission of erroneous data. As mentioned above, these fines could correspond to a maximum amount of up to **EUR 80 million** per year.

Table 3: Summary of costs implications, per policy option (in EUR million)

		Airline industry*		***Member States***		***eu-LISA***	
		One-off	*Recurrent*	*One-off*	*Recurrent*	*One-of*	*Recurrent*
Option 1.1** ***Inbound extra-Schengen flights***		0	– 2,53	13,5	0	34	1.4
Combined with…	***Option 2.1*** *inbound and outbound extra-EU flights*	0	4,21	0	0		
	Option 2.2 *inboud, outbound extra-EU and intra-EU and domestic flights*	75	20,35	0	0		
Option 1.2** ***Outbound extra-Schengen flights***		0	1,68	67.5	0		
Combined with…	***Option 2.1*** *inbound and outbound extra-EU flights*	0	0	0	0		
	Option 2.2 *inboud, outbound extra-EU and intra-EU and domestic flights*	75	16,13	0	0		
Option 3.1		0	n.a.	n.a.	n.a	n.a	n.a.
Option 3.2		50	n.a.	n.a	n.a.	n.a	n.a.

** Due to limited availability of data, the assumptions and calculations include costs for both scheduled and non-scheduled air carriers.*

*** ** The reported net costs of the different policy options for law enforcement (2.1 and 2.2) depend on the choice made for border management (1.1 or 1.2.) Therefore both options 2.1 and 2.2 are reported twice: once under the option 1.1, and a second time under option 1.2. For instance, if option 1.2 and option 2.2 were chosen, net costs for the airline industry would amount to EUR 1,61 million for border management and EUR 27,05 million for law enforcement.*

6.3. Fundamental rights, including the protection of personal data

The policy options described in section 5.2 provide for the processing of personal data of passengers and hence limit the exercise of the fundamental right to the **protection of personal data** as guaranteed by Article 8 of the Charter and Article 16 of the TFEU. As underlined by the CJEU,[86] the right to the protection of personal data is not an absolute right, but any limitation must be considered in relation to its function in society and comply with the criteria set out in Article 52(1) of the Charter.[87] Personal data protection is also closely linked to respect for **private and family life** protected by Article 7 of the Charter. Policy option 2.2 provides for the collection of data linked to cross-border travel within the EU, and hence could deter the exercise of the right to **freedom of movement** as guaranteed by Article 45 of the Charter.[88] As with the right to the protection of personal data, any limitation of the exercise of the right to freedom of movement must comply with the criteria set out in Article 52(1) of the Charter. Furthermore, account should be taken of the **freedom to conduct a business**, enshirened in Article 16 of the Charter, wherer policy options 2.2, 3.1 and 3.1 would impose new obligations on air carriers that could deter the exercise of their freedom to conduct a business. This, too, is a fundamental right the exercise of which may be limited in accordance with Article 52(1) of the Charter.

Consequently, in so far as they limit the exercise of fundamental rights such as those mentioned above, the policy options need to comply with the conditions set out in Article 52(1) of the Charter. The opportunities offered by the policy options presented need to be balanced with the obligation to ensure that any limitation of the exercise of fundamental rights that may derive from them respects the essence of those rights and remains limited to what is strictly necessary to genuinely meet the objectives of general interest recognised by the EU pursued, subject to the principle of proportionality.

Both the objectives of ensuring effective border controls and of effectively combating serious crime and terrorism are objectives of general interest within the meaning of Article 52(1) of the Charter. Furthermore, there is no reason to consider that the essence of the fundamental rights at stake would not be respected. Accordingly, this chapter will assess the policy options focusing on the requirements of necessity and proportionality.[89]

Policy option 1.1 – *API data collection on all extra-Schengen inbound flights*

Right to the protection of personal data

Necessity: The obligation to collect and process API data on all inbound flights to the Schengen area would effectively respond to the objective of ensuring that pre-checks are carried out on all air passengers travelling to the Schengen area.

---

[86] CJEU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-0000.

[87] In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

[88] CJEU, judgment of 21.6.2022, Case C-817/19, *Ligue des droits humains*, paragraphs 278-279.

[89] European Data Protection Supervisor (EDPS), Assessing the necessity of measures the limit the fundamental right to the protection of personal data: a toolkit (April 2017); EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (December 2019); Fundamental Rights Agency, Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level (2018).

In terms of alternative approaches, the collection of API data for external border management based on national risk assessments – i.e. only on selected flights – would be less intrusive on the right to the protection of personal data as less data subjects would be affected. However, this approach would not respond effectively to the objective pursued to enhance pre-checks at external borders as it would risk missing out on hits, alerts or other security threats at external borders. Non-legislative measures such as recommendations or best practices would also not be an effective means to achieve the objective as the current framework does not oblige Member States to collect API data.

Consequently, the policy option is limited to what is strictly necessary to achieve the above mentioned objective. It covers all passengers crossing the external borders upon entry to respond to the need for a coordinated approach to the management and security of external borders. While no decisions will be taken by competent border authorities solely based on API data or the results of the cross-checks with other databases, this policy option effectively enables border authorities to organise their activities in advance and facilitate the entry of bona fide passengers. To do so, API data collected must be limited to information contained in the passenger's passport, all of which are necessary to carry out pre-checks upon arrival at the borders against those databases set out in the Schengen Borders Code.

Proportionality: This policy option affects all passengers who are travelling by air to the Schengen area. This constitutes additional data subjects affected compared with the current situation where API data is collected only on a share of those passengers.

The policy option does not impose a disproportionate burden on the persons affected by this option. The interference with the right to the protection of personal data is limited to what is strictly necessary to achieve the objective of pre-checks of persons prior to their arrival at external borders.. Limiting the passenger's identity data to information contained in the passenger's passport constitutes an important safeguard and an improvement to the current rules which allow for additional data to be collected from passengers.

Policy option 1.2 – *API data collection on all extra-Schengen inboud and outbound flights*

Right to the protection of personal data

Necessity: This option would address an objective of general interest, namely to enhance EU border management by ensuring that every person crossing the Schengen external borders – at arrival and departure – is pre-checked. However, as the full API data set is generated once the passengers are on board of a plane, on outbound flights, the border guards would only receive the API data after the physical exit checks of the travellers and examination of their passports, and hence too late to support the work of the border guards. Consequently, the policy option does not effectively respond to the objective. As a result, **the policy option does not pass the necessity test**, and will therefore not be assessed in terms of its proportionality.

Policy option 2.1 – *API data collection for law enforcement purposes on all extra-EU inbound and outbound flights*

Right to the protection of personal data

Necessity: This policy option is genuinely effective to achieve the specific objective of effectively fighting serious crime and terrorism and hence enhance internal security, as it allows for the joint processing of API data and PNR data for flights entering and leaving the

EU. In doing so, this policy option improves the quality of the data processed by Passenger Information Units and hence significantly reduces the risk of false matches due to data quality issues.[90] This option also provides additional legal certainty regarding the criteria for the collection and transmission of API data for law enforcement purposes.

The purposes of the processing of API data would be for the prevention, detection, investigation and prosecution of serious crimes as defined by the PNR Directive. This requires the processing of the same set of API data as those collected for border management purposes, i.e. information contained in the passenger's passport, as this data is necessary to identify the traveller and to confirm the travel and flight details.

Alternatives to this policy option would be less effective to achieve the objective of fighting serious crime and terrorism with API data complementing PNR data. The collection of API data only on selected extra-EU flights would imply that competent law enforcement authorities would not be able to combine API and PNR data for all passengers, thus maintaining the risk of security gaps on flights coming to or departing from the EU. Consequently, this policy option is limited to what is strictly necessary to achieve the above mentioned objective.

Proportionality: This policy option provides uniform criteria for the collection and transmission of API data for law enforcement purposes on EU inbound and outbound flights, responding effectively to a need identified in section 2.2 and solving part of the problem resulting from the absence of EU-wide rules on the collection and use of API data for law enforcement purposes.

To limit the interference of this policy measure on the rights of passengers to what is strictly necessary, a number of safeguards are required: First, the processing of API data by Passenger Information Units must be restricted to a closed and limited list of API data from air carriers to fight terrorism and serious crime, i.e. to the data contained in the passenger's passport. Beyond that, no additional identity data shall be collected from passengers. Second, the further processing of the API data by the Passenger Information Unit, by way of joint processing of API with PNR data, must comply with the provisions of the PNR Directive as interpreted by the ruling of the CJEU in the *Ligue des droits humains* case, including on the retention period of the data, access to data and safeguards on the processing of data when cross-checked with other databases.

Weighing up the intensity of the interference with the fundamental right to the protection of personal data with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest of EU law, the policy option constitutes a proportionate response to the need to solve the problem resulting from a lack of joint processing of API and PNR data on extra-EU inbound and outbound flights.

Policy option 2.2 – *API data collection for law enforcement purposes on all extra-EU flights, intra-EU and domestic flights for which PNR data is collected*

Right to the protection of personal data

[90] See Fundamental Rights Agency (2018): Submission to the CJEU in Case C-817/19, paras. 14-21; Fundamental Rights Agency (2018): Legal opinion on interoperability and fundamental rights implications, pp. 37-38.

Necessity: The policy option is genuinely effective to achieve the specific objective of effectively combatting serious crime and terrorism and hence enhancing internal security, as it allows for the joint processing of API data and PNR data for extra-EU, intra-EU and domestic flights. In doing so, this policy option improves the quality of the data processed by Passenger Information Units and hence significantly reduces the risk of false positive matches due to data quality issues.[91] This policy option also provides the necessary legal clarity and foreseeability concerning the collection and transmission of API data. It sets clearer requirements regarding the purpose of the collection which are limited to the purposes of the PNR Directive. The collection of API data would be limited to flights where PNR data is collected and processed, and hence to selected intra-EU and domestic flights.

As with policy option 2.1, the purposes of the processing of API data would be the prevention, detection, investigation and prosecution of serious crimes as defined by the PNR Directive. This requires the processing of the same set of API data as those collected for border management purposes, i.e. information contained in the passenger's passport, as this data is necessary for the Passenger Information Unit to identify the traveller and to confirm the travel and flight details.

In terms of alternatives, the policy option is less intrusive than the systematic collection on all intra-EU flights, i.e. including also flights for which PNR data is not collected, which is a discarded policy option (see section 5.3). Non-legislative measures would not be effective to achieve the specific objective as a legal requirement is necessary to oblige air carriers to collect API data. Existing practices such as conformity checks, i.e. comparing a passenger's name on the boarding pass and travel document before boarding, are not effective to achieve the objective of obtaining reliable data on passengers taking a flight (see section 2.2). Consequently, the policy option is limited to what is strictly necessary to achieve the above mentioned objective.

Proportionality: This policy option correspond to an identified need to enhance internal security. This measure effectively responds to the problem resulting from the absence of joint processing of API and PNR data on intra-EU flights.

To limit the interference of this policy option on the rights of passengers to what is strictly necessary, a number of safeguards are required. First, the processing of API data by Passenger Information Units must be restricted to a closed and limited list of API data from air carriers to fight terrorism and serious crime, i.e. to the identity data contained in the passenger's passport. Beyond that, no additional identity data shall be collected from passengers. Second, while the CJEU held in the *Ligue des droits humains* case that the collection and processing of PNR data from passengers is a serious interference to the right of personal data protection, articulated a set of requirements and detailed safeguards within which the Court considered that it would be proportionate to collect and process PNR data on selected intra-EU flights. Under this policy option, the processing of API data must follow the same requirements and safeguards (see section 5.2.2), i.e. those resulting from the provisions of the PNR Directive as interpreted by the CJEU in the *Ligue des droits humains* case, including on the retention period of the data, access to data and safeguards on the processing of data when cross-checked with other databases.

[91] See Fundamental Rights Agency (2018): Submission to the CJEU in Case C-817/19, paras. 14-21; Fundamental Rights Agency (2018): Legal opinion on interoperability and fundamental rights implications, pp. 37-38.

Weighing up the intensity of the interference with the fundamental right to the protection of personal data with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest of the EU, the policy option constitutes a proportionate response to the need to solve the problem resulting from a lack of joint processing of API and PNR data on intra-EU flights. This policy option is proportionate as the obligation on the air carrier to collect and transmit API data would not be systematic for all intra-EU and domestic flights. Instead, it would be based on a threat assessment that the Member States carry out, in line with the requirments set by the ruling of the Court of Justice in the *Ligue des droits humains* case, when they select the flights for which they request PNR data. Consequently, the obligation on the air carrier to collect and transmit API data would be limited to flights for which PNR data is collected. The API router would provide a technical solution to limit the transfer of API data to selected flights only (see Annex 7).

Right to freedom of movement

This policy option also affects the right to freedom of movement as it would imply the processing of API data for selected intra-EU and domestic flights. To limit the interference of this policy option on the right to freedom of movement to what is strictly necessary, a number of safeguards are required. While the CJEU stated in the *Ligue des droits humains* case that the collection and processing of PNR data from passengers linked to the cross-border travel could deter the exercise of the right to freedom of movement, it also provided guidance on the extent to which passenger data could be collected in a manner that is limited to what is strictly necessary to achieve the intended objective thereby ensuring respect for the principle of proportionality. Under this policy option, the processing of API data must follow the same requirements and safeguards set out by the CJEU (see section 5.2.2).

Moreover, this interference is balanced by the possibility left to passengers to provide their API data free of charge at a check-in desk, a self-service kiosk or during boarding at the airport if they do not wish or cannot use devices such as smartphones or webcams to check-in online. This safeguard would ensure that airline staff would be available if needed to use automated means (smartphone, webcam, or other devices reading the MRZ) on behalf of the passenger to collect the API data. This would cater for any inequality in treatment for passengers not having access to smartphones. It would therefore ensure compliance with the requirement of non-discrimination under the Charter in the context of the right to freedom of movement. As an additional safeguard, the collection of API data on selected intra-EU and domestic flights can only include the requirement for air carriers to collect passenger information and not the obligation for air carriers to verify the information on the basis of an identity check or correspondence of the identity with the boarding pass.

Weighing up the intensity of the interference with the fundamental right to freedrom of movement with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest of the EU, the policy option constitutes a proportionate response to the need to solve the problem resulting from a lack of joint processing of API and PNR data on intra-EU and domestic flights. This policy option is proportionate as the obligation on the air carrier to collect and transmit API data would not be systematic for all intra-EU and domestic flights. Instead, it would be based on a threat assessment by the Member States when selecting the flights for which they request PNR data, and hence limited to flights for which PNR data is collected. The API router would provide a technical solution to limit the transfer of API data to selected flights only (see Annex 7).

Freedom to conduct a business

This policy option also affects the freedom to conduct a business for air carriers operating on intra-EU flights as those air carriers do not yet collect passenger API data on these flights for the transmission to Member States.

This interference is limited to situations where Member States request such data for legitimate purposes, namely for the fight against serious crime and terrorism. Importantly, the financial burden on air carriers resulting form that interference would be rather marginal compared to their total turnover.[92] Consequently, the essence of the freedom to conduct a business is not affected by the policy option.

Policy option 3.1 – *API data collection by either automated or manual means*

Right to the protection of personal data

Necessity: This policy option is a horizontal and technical measure to enhance the reliability and verified nature of API data (i.e. that the data collected corresponds to the passenger boarding a plane and to information featuring on the MRZ of the travel document), contributing to the effectiveness of the three objectives mentioned in section 4. A higher quality of API data transmitted lowers the risk for competent authorities of missing information on a person who represents a threat and for whom additional analysis could be carried out. In doing so, this policy option also improves the quality of the data and hence reduces the risk of false matches due to data quality issues.[93] Consequently, this policy option increases the effectiveness of competent authorities both in respect of the objective of border controls and that of tackling serious crime and terrorism.

Current measures, as described in section 2, are not sufficient to ensure that the API data transmitted to authorities accurately includes the information contained in a passenger's travel document. While the MRZ is an internationally agreed standard, the current legal framework does not specify from which sources API data should be collected nor how it should be collected. Alternative measures, in the form of guidelines or recommendations adopted at EU level, would not achieve the needed level of harmonisation to ensure that the same set of data is collected from passengers and transmitted to national authorities. This option further eliminates less effective practices to ensure the reliability of API data such as conformity checks on flights where only PNR data was collected (see section 2.2). However, as this policy option provides for a wide range of methods to collect the data from passengers (either online or at the desk of airlines), it maintains part of the risk that the API data transmitted to authorities would not accurately include the information contained in a passenger's travel document.

Proportionality: The measure would apply to all passengers, regulating the collection of API data, i.e. the data contained in the passenger's passport.

The interference to the right of protection of personal data and their private life of passengers is mitigated by the fact that the option clarifies which personal data is collected from passengers. In line with the necessary safeguards identified for policy options 1.1, 2.1

[92] In 2019, total turnover of the air transport was of EUR 1 285 billion according Eurostat data, retrieved on 27 July 2020 from [sbs_sc_sca_r2] data set.
[93] See Fundamental Rights Agency (2018): Submission to the CJEU in Case C-817/19, paras. 14-21; Fundamental Rights Agency (2018): Legal opinion on interoperability and fundamental rights implications, pp. 37-38.

and 2.2, no additional data shall be collected from passengers. The level of the interference of the measure is also balanced by the fact that the collection of the data in this option concerns a wide range of methods to collect the data from passengers (either online or at a check-in desk, a self-service kiosk or during boarding at the airport), without additional fees for passengers when chosing online or traditional check-in. This would cater for any inequality in treatment for passengers with limited digital literacy or with a different social or economic backround, not having access to smartphones. It would therefore ensure compliance with the requirement of non-discrimination under the Charter, including in the context of exercising the right to freedom of movement.[94] Where airline staff would collect API data on behalf of the passengers, EU standards set by the General Data Protection Regulation and the related safeguards would apply.

Freedom to conduct a business

This option also affects the freedom to conduct a business (Article 16 of the Charter) of air carriers, particularly for those companies carrying passengers on intra-EU flights as those air carriers do not yet collect API data on these flights for the tramission to Member States. This interference is limited to situations where Member States request such data for legitimate purposes. This measure would affect the freedom in a proportionate manner as air air carriers would have several options to comply with the obligation to collect API data from passengers, and would retain the flexibility to implement solutions to collect API data from passengers in line with their business model. Consequently, the essence of the freedom to conduct a business is not affected by the policy option.

Policy option 3.2 – *API data collection by automated means only*

Right to the protection of personal data

Necessity: This policy option genuinely contributes to the effectiveness of the three objectives mentioned in section 4. The mandatory collection of API data by automated means - meaning the optical character recognition of a travel document's MRZ by a device (smartphone, webcam, or other devices reading the MRZ) will significantly enhance the quality and reliability of API data collected by air carriers. It will drastically reduce the risks of transmitting API data containing errors in what constitutes the core of the information, meaning information on the travel document and identity of the passenger. Automated means to collect API data will also support better processing of API data by improving the quality of the data and reducing significantly the risk of false matches due to data quality issues.[95]

In terms of alternative measures, leaving the option to air carriers to collect API data either by manual or automated means – as assessed in policy option 3.1 – would be less effective in responding to the need for accurate and reliable API data. Maintaining manual means would leave the option to air carriers to continue with the practice of manually 'self-declared' API data by passengers which is a more error-prone method.

Policy option 3.2 would no longer allow for any manually ‘self-declared’ API data. It would be limited to what is strictly necessary to achieve the above mentioned objective. Where

[94] Linked to policy option 2.2. where impact on the free movement was assessed.
[95] See Fundamental Rights Agency (2018): Submission to the CJEU in Case C-817/19, paras. 14-21; Fundamental Rights Agency (2018): Legal opinion on interoperability and fundamental rights implications, pp. 37-38.

airline staff would collect API data on behalf of the passengers, EU standards set by the General Data Protection Regulation and the related safeguards apply.

Proportionality: The measure would apply to all passengers, regulating the collection of API data, i.e. the identity data contained in the passenger's travel document.

The use of automation can lead to additional risks from the viewpoint of the protection of personal data. However, the possibility would be left to passengers to provide their API data free of charge at a check-in desk, a self-service kiosk or during boarding at the airportif they do not wish or cannot use devices such as smartphones or webcams to check-in online. This safeguard would ensure airline staff would be available if needed to use automated means (smartphone, webcam, or other devices reading the MRZ) on behalf of the passenger to collect the API data. This would cater for any inequality in treatment for passengers with limited digital literacy or with a different social backround, not having access to smartphones. It would therefore ensure compliance with the requirement of non-discrimination under the Charter, including in the context of exercising the right to freedom of movement.[96] Nonetheless, in view of those risks, the necessary additional safeguards would be provided for, including as regards security, accuracy and the exercise of data subjects rights, in line with the EU standards required by the General Data Protection Regulation and the Law Enforcement Directive.[97]

Weighing up the intensity of the interference with the fundamental right to the protection of personal data with the legitimacy of the objectives of border management and the fight against serious crime and terrorism as objectives of general interest of the EU, the policy option constitutes a proportionate response to the need to enhance the quality and reliability of API data.

Freedom to conduct a business

This option also affects the freedom to conduct a business of air carriers, particularly for those companies carrying passengers on intra-EU flights as those air carriers do not yet collect passenger API data on these flights for the tramission to Member States.

Moreover, some air carriers make the online check-in mandatory for their passengers. This policy option would require air carriers to change such practices, as passengers not willing or able to scan their travel document electronically must have the possibility under this policy option to provide their API data at a check-in desk, a self-service kiosk or during boarding at the airport (see above on the right to freedom of movement).

This interference is limited to situations where Member States request such data for legitimate purposes. Moreover, the financial burden on air carriers resulting from the interference would be rather marginal compared to their revenue.[98] Consequently, the essence of the freedom to conduct a business is not affected by the policy option.

[96] Linked to policy option 2.2. where impact on the free movement was assessed.
[97] See Fundamental Rights Agency (2014): Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data, para. 8; Fundamental Rights Agency (2018): Legal opinion on interoperability and fundamental rights implications, pp. 45-54; Fundamental Rights Agency (2017): Legal opinion on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS), pp. 41-44.
[98] Air transport total turnover in 2019 amounts to EUR 1 285 billion; Eurostat data, retrieved on 27 July from [sbs_sc_sca_r2] data set.

7. HOW DO THE OPTIONS COMPARE?

This chapter compares each option against the baseline scenario (i.e. where no action is taken for that policy option).

To determine the preferred options, all policy options identified in section 5.2 have been assessed and compared in light of the following criteria:

- effectiveness, i.e. the extent to which the option meets the policy objectives;
- efficiency, i.e. the relative weight of the costs and benefits of the option;
- level of impact on fundamental rights, including protection of personal data.

The result of the comparison for all criteria are provided for each instrument with an overview table. The scoring ranges from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores – 'positive impact' ('+'), 'neutral' (0) and 'negative impact' (-).

The comparison of policy options is presented according to each envisaged instrument and purpose that would replace the current API Directive, i.e. for the envisaged API instrument for Schengen external border management and for the envisaged API instrument for law enforcement purposes. The cross-cutting policy options on API data collection are applicable to both purposes.

7.1. API instrument for Schengen external border management

Policy option *Assessment criteria*	**1.1. API data collection on all extra-Schengen inbound flights**	**1.2. API data collection on all extra-Schengen inbound and outbound flights**	**3.1. API data collection by either automated or manual means**	**3.2. API data collection by automated means only**
Effectiveness				
Enhance advance checks at external borders	++	0	+	++
Facilitate the flow of bonafide travellers at the external borders	++	0	0	–
Efficiency				
Member States	–	– –	N/A	N/A
Air carriers	0	–	0	–
Fundamental rights	0	–	0	0
Preferred policy options	**X**			**X**

Policy options 1.1 and 3.2 are the preferred policy options for the processing of API data for Schengen external border management.

Effectiveness. By establishing a clear obligation on Member States to collect and process API data on all travellers coming to the Schengen area, **policy option 1.1** would most effectively respond to the objectives of pre-checks prior to arrival at external borders and speed-up the clearance of low-risk passengers. Option 1.1 would bring legal clarity that API data should be collected on all incoming flights. It would also provide the framework for a consistent approach among competent border authorities for the use of API data for pre-

checks of all travellers before they enter the Schengen area. **Option 1.2** contributes to these objectives to the extent that border guards would receive API data prior to arrival but also after the passengers have boarded the plane and after border guards physically checked their travel documents. Accordingly, option 1.2 would have no impact on the facilitation of travellers at exit.

Option 3.1 would contribute positively to the objective of enhancing pre-checks upon arrival at external borders by setting more transparent criteria on the source of API data (i.e. collected from the MRZ of passengers' travel documents). Option 3.1 would not change the means of collection of API data compared to existing practices of air carriers, therefore having a neutral impact on the facilitation of travellers. Option 3.1 would also include a more transparent criteria on the sanctions which could be incurred by air carriers in case of errors in the transmission of API data, which would have some impact on the quality of the data transmitted. However, the manual entry of information would still remain possible, with a higher risk of errors that such approach entails. For this reason, the collection of API data using automated means only as proposed in option 3.2 is preferred. **Option 3.2** would provide an increased certainty around the accurateness and completeness of the data collected and therefore would contribute more effectively to the objective of enhancing pre-checks at external borders. The impact on facilitation of option 3.2 is deemed negative as it reduces the number of ways for travellers and airlines to collect and capture API data.

Efficiency. For *Member States*, policy **option 1.1** is more efficient than **option 1.2**, the latter would imply more significant adaptations to their systems to collect API data on both inbound and outbound flights. Policy options 3.1. and 3.2 do not imply additional costs for national authorities and therefore the efficiency for Member States is not assessed. National authorities would benefit from more accurate and reliable data under **policy option 3.2**, with less time and resources spent on verifying errors in transmission of data. It should be noted that such benefits could not be quantified by Member States.

On inbound travels, the share of passengers on which API data is collected is currently estimated at around 65%, a systematic collection of API data on all flights and passengers in **option 1.1** would involve additional costs for Member States to upgrade their systems to receive and process additional passenger data. Such costs would however be higher if API data were to be collected on inbound and on outbound travels (**policy option 1.2**), as the estimates on the share of passengers on which API data is currently collected on outbound flights are lower (around 25%).

Likewise, *airlines* would have an obligation to transmit API data systematically on all inbound flights in **option 1.1**. The transmission costs would be mitigated by the fact that air carriers would transmit the API data only once to the carrier interface (accompanied by the API router), instead of multiple times to Member States. Over time, this single transmission would result in cost savings for the airline industry. While some airlines operating flights to third countries are currently also collecting API data on these flights (policy **option 1.2**), this is not the case for all airlines nor on all outbound flights, and likely not following the same criteria as those set by Member States. Therefore, as assessed in section 6, **option 1.2** would imply additional costs, with higher costs than in policy option 1.1.

Compared to policy option 3.1 where airlines would retain flexibility concerning the means to collect API data from passengers, airlines would incur additional costs for the implementation of policy **option 3.2**, and arguably the most significant costs. Cost-savings on the medium term for airlines would be possible in option 3.2 as a result of a reduced exposition to sanctions for non-compliance and transmission of erroneous data.

Whereas airlines would also benefit from clearer and similar requirements for the collection of API data, such benefits could not be quantified. In more qualitative terms, standard requirements in policy options 1.1 and 1.2. would mean greater compliance and less need to spend human resources for air carriers to determine for which flights they should transmit API data to Member States, and which data elements.

Smaller air carriers, such as business aviation or charter flights which transport a smaller number of passengers, and for which the implementation of a dedicated system to collect and transmit API data could represent an additional burden, would have the possibility to do so via different means. For example a web-portal might be more suitable to their business model, a solution which is already available and does not need additional investments. Such a solution would also be made available by national authorities and eu-LISA when developing the carrier interface and the API router.

Fundamental rights, including the protection of personal data. As per the assessment in section 6 on the impact on the protection of personal data, API data collection would be limited to what is necessary and would be proportionate for border management purposes in policy **option 1.1**, while the necessity test would not be met for policy **option 1.2**.

Policy **options 3.1 and 3.2** would both increase the legal certainty of the data processed by competent border authorities. The collection of API data from the MRZ fields of travel documents is the same data to which border guards have access when looking at passengers' travel documents at the check at the external border.

In policy **option 3.2**., the use of automated means only for the capture of API data from passengers can lead to additional risks from the viewpoint of the protection of personal data of passengers. Therefore, this option would need to include effective safeguards to ensure that airline staff would be available where needed to collect API data on behalf of passengers, in line with the EU standards set by the General Data Protection Regulation and the related safeguards.

7.2. API instrument for law enforcement purposes

Policy option *Assessment criteria*	**2.1. API data collection on all extra-EU inbound and outbound flights**	**2.2. API data collection on all extra-EU, intra-EU and domestic flights for which PNR data is collected**	**3.1. API data collection by either automated or manual means**	**3.2. API data collection by automated means only**
Effectiveness				
Effectively combat serious crime and terrorism with API data complementing PNR data	+	++	+	++
Efficiency				
Member States	0	0	N/A	N/A
Air carriers	–*	– –	0	–
Fundamental rights	0	0	0	0
Preferred policy options		**X**		**X**

** Costs estimated for air carriers for policy option 2.1 are similar to the costs estimated for policy option 1.2.*

Policy options 2.2 and 3.2 are the preferred policy options for the processing of API data for law enforcement purposes.

Effectiveness. Policy option 2.1. would positively contribute to the objective of effectively combating serious crime and terrorism in the EU as it would allow for the joint processing of API data and PNR data of all passengers on flights entering and leaving the EU. However, this option would leave a significant gap on the joint processing of API and PNR data on flights within the EU and would only partially solve the problem identified in Chapter 2.

Compared to policy option 2.1, **policy option 2.2** would contribute more effectively to the objective of combating serious crime and terrorism in the EU as it would allow for the joint processing of API data and PNR data on all passengers travelling to, from and within the EU. This option would enhance the effectiveness of PNR data as a tool to fight serious crime and terrorism as it would clarify the purposes of API data processing for law enforcement, and as it would provide EU-wide criteria (type of flights, data collected) upon which air carriers would need to collect API data and transmitted it to Passenger information Units. The joint processing of API data and PNR data would enable Passenger Information Units to enhance the quality and reliability of the matches in databases of known suspects, as well as to confirm the travel history of suspects (e.g. also keeping informed the third country of destination where relevant). To the extent that PNR data is transmitted to Member States on intra-EU and domestic flights, this policy option would also set a new obligation on Member States to require air carriers to collect and transmit API data on the same selected flights. In that regard and compared to policy option 2.1., this option would close an important gap in the processing of API data by the Passenger Information Units, as it would allow the joint processing of API data and PNR data – as a very effective law enforcement tool – for all flights for which Member States request air carriers to transmit PNR data. This option would therefore have a very positive impact on achieving the specific objective to effectively combat serious crime and terrorism and enhance internal security. The contribution of policy option 2.1 to the specific objective is therefore very positive.

As regards the collection of API data, the processing of such data for law enforcement purposes requires high quality data and with as few errors as possible. Only verified API data, collected by automated means, allow for an effective use of the joint processing of API data and PNR data in the fight against serious crime and terrorism.For this reason, **policy option 3.2** is the preferred policy option for the collection of data, as it is contains a much lower risk of erroneous data being transferred to Passenger Information Units compared to policy option 3.1.

Efficiency. It is estimated that *Member States* (i.e. their Passenger Information Units) would not incur additional costs for the processing of additional API data in policy policy options 2.1 and 2.2. Hence the impacts of both policy options 2.1 and 2.2 are neutral in terms of additional costs. Moroever, as a result of the joint processing of API data and PNR data, Passenger Information Units would benefit from increased analysis capabilities, due to the increased quality of data (API as confirmed information v. PNR as declaratory information), with less resources spent to check matches resulting from the automated comparison with relevant databases (e.g. Schengen Information System). Member States' practiontioner reported that the availability of the full API dataset, including the birth date and the

passengers' travel document number, drastically reduces 'false-positive' matches resuling from the automated processing of PNR data against relevant databases. This makes the overall processing of passenger data much more efficient and less intrusive for passengers.[99] Such benefits of the joint processing of API data and PNR data could not be further quantified by Member States.

From the *airline* industry perspective, the costs for **policy option 2.1** are considered similar to those of policy option 1.2. As in policy option 1.2, air carriers would transmit API data under policy option 2.1 only once to the carrier interface (accompanied by an API router), and hence no longer require connections to 27 separate Passenger Information Units.

Building on the cost estimations of policy option 1.2 and 2.1, **policy option 2.2** would mandate airlines to transmit API data on selected intra-EU and domestic flights, which would represent an additional and new cost for air carriers compared to policy option 2.1. They would need to upgrade their IT system or invest in a new IT system (departure control system) to be able to collect and transmit API data. This one-off cost was estimated at a maximum of **EUR 75 million**.

To an extent, the costs for policy option 3.1 and 3.2 are similar for air carreirs, irrespective of whether the technology to capture API data would be implemented for external border management or for law enforcement purposes.

Fundamental rights. While regulating the collection of API data on different types of flights, policy options 2.1 and 2.2 would both improve the quality of the data processed by the Passenger Information Units. Both policy options would provide legal certainty regarding the criteria for the collection and transmission of API data in terms of the purposes for the collection and data set to be collected from passengers. As regards the further processing of API data by the Passenger Information Unit, by way of combined processing of API data with PNR data, both policy options would need to comply with the provisions of the PNR Directive as interpreted by the ruling of the CJEU in the *Ligue des droits humains* case. This would include the retention of the data period, access to data and safeguards on the processing of data.

While regulating the collection of API data on different type of flights, **policy options 2.1 and 2.2** would both improve the quality of the data processed by the Passenger Information Units. Both policy options also provide legal certainty regarding the criteria for the collection and transmission of API data in terms of the purposes for the collection and data set to be collected from passengers. As regards the further processing of API data by the Passenger Information Unit, by way of combined processing of API with PNR data, both policy options would comply with the provisions of the PNR Directive as interpreted by the ruling of the Court of Justice in the *Ligue des droits humains* case. This includes the retention of the data, access to data and safeguards on the processing of data.

To ensure that the collection and further processing of API data on intra-EU and domestic flights does not interfere with the rights of passengers, including their right to free movement, equality in treatment and non-discrimination, **policy options 2.2 and 3.2** are accompanied by a number of safeguards for passengers who do not wish or cannot use devises to check-in online using automated means. These include providing API data free-of

[99] SWD(2020) 128 final, p. 43 and and targeted stakeholder consultations with national technical experts.

charge at the check-in desks at the airport and ensuring presence of airline staff to collect API data by automated means on behalf of the passenger.

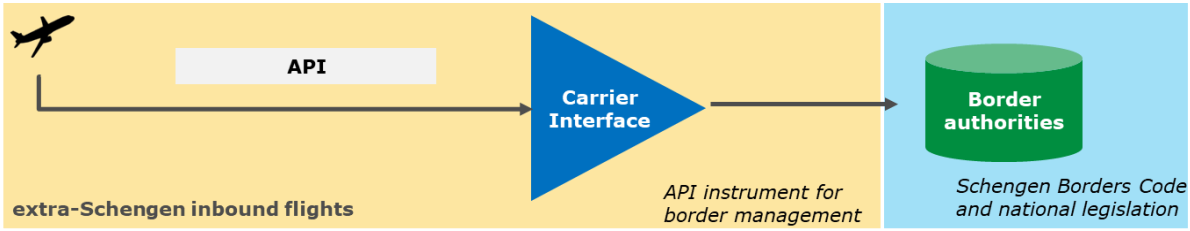
8. PREFERRED OPTION

The preferred option is a combination of policy options, namely a combination of API data collection on extra-Schengen inbound flights for external border management (policy option 1.1), on extra-EU inbound and outbound flights, intra-EU and domestic flights for law enforcement purposes (policy option 2.2). The obligation to transmit a complete API data set by air carriers using automated means only (policy option 3.2) would apply for both external border management and for law enforcement purposes.

Taken together, the preferred policy options assessed in section 6 would reinforce the current framework for the collection and use of API data for **Schengen external border management** on the one hand and **law enforcement purposes** on the other. This chapter presents the accumulated impact of the preferred options as per instrument and purpose for the use of API data.

8.1. Preferred option for the collection of API data for border management purposes

Chart 2: Overview of use of API data for Schengen external border management



The combined effects of policy options 1.1 and 3.2 would strengthen the API data as an instrument enchancing the pre-checks of travellers at Schengen external borders. The preferred policy options would set an obligation on Member States to request air carriers to collect and transmit API data for all flights entering the Schengen area, in alignment with international standards and recommended practices. They would also establish clear criteria on what constitutes an API data set, on which flights API data should be collected and on the processing rules to be applied, hence establishing a consistent approach to the use of API data for external border management across Member States bound by the Schengen *acquis*. Competent border authorities would use API data in accordance with the applicable provisions of EU law, notably on the protection of personal data and the Schengen Borders Code, and national legislation on entry checks in compliance with EU law.

The standardisation of API requirements for external border management across Member States would also bring further benefits, such as increased compliance by air carriers. They would need to transmit API data only to the carrier interface, which would then distribute the data to the relevant competent authorities with the API router. The carrier interface would also reduce the costs for air carriers for API data transmission. It would also reduce the human resources needed by competent border authorities as they would no longer need to maintain separate connections with each air carrier transporting passengers to its territory.

A strengthened API instrument for pre-checks upon arrival at Schengen external borders would provide competent border authorities with more reliable and verified API data, as that

data would be retrieved from the travel documents of passengers by automated means only. As a result, competent border authorities would have an effective tool to ensure a speedier facilitation or clearance of passengers upon disembarkation.

The costs of an API instrument for border management purposes are summarised in the table below. The costs incurred by eu-LISA for the establishment of the API router capability to the existing carrier interface (see also Annex 7) would be counted only once. These costs implications are expected to be applicable as of the next multiannual financial framework, in 2028. Table 4 below summarises the costs for each stakeholder group.

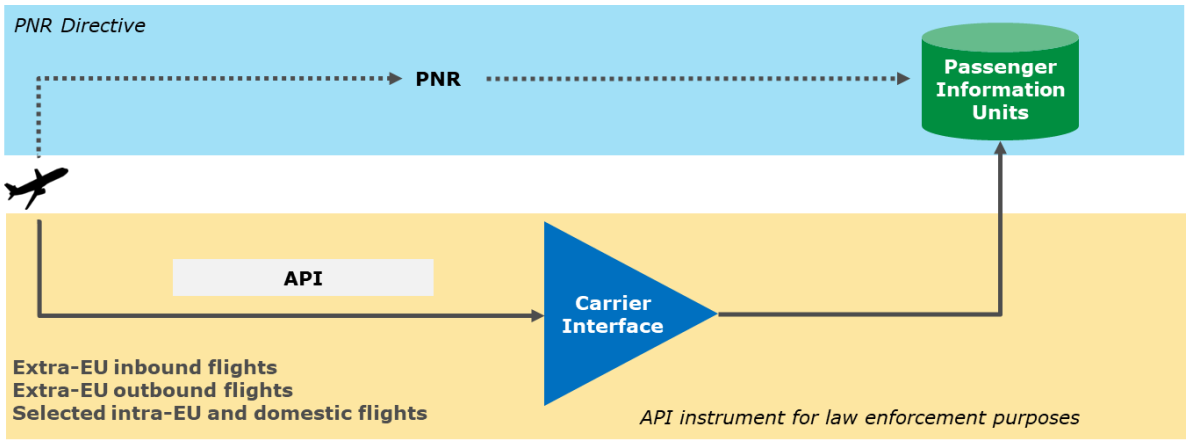
Table 4: Overview of costs for an API instrument for border management purposes (in EUR million)

	Airline industry*		***Member States***		***eu-LISA***	
	One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
Option 1.1	0	– 2,53	0	13,5	34	1.4
Option 3.2	50	n.a.	n.a	n.a.	n.a.	n.a.

** Due to limited availability of data, the assumptions and calculations include costs for both scheduled and non-scheduled carriers*

8.2. Preferred option for the collection of API data for law enforcement purposes

Chart 3: Overview of use of API data for law enforcement purposes



A separate API instrument for law enforcement purposes would regulate the API data collection on all flights into and outside the EU, as well as on selected intra-EU and domestic flights for which PNR data is transmitted. The combined effects of policy options 2.2 and 3.2, and more specifically the joint processing of API data and PNR data on all flights where PNR data is requested by Member States, would significantly reinforce the robustness of the PNR Directive in the fight against serious crime and terrorism. Passenger Information Units would benefit from higher quality and verified API data to identify persons involved in serious crime or terrorism.

The transmission of API data for law enforcement purposes would build on the capabilities developed for the transmission of API data to the carrier interface for external border management, with no additional costs for eu-LISA. Again, air carriers would need to

transmit API data only to the carrier interface, which would then deliver the data to the Passenger Information Unit of each Member State concerned. This would be a cost-efficient solution for air carriers and would reduce part of the transmission costs. However, air carriers would need to collect and transmit additional API data, as the preferred policy options include selected intra-EU and domestic flights for which PNR data is collected. Table 4 below summarises the costs for each stakeholder group.

Table 5: Overview of costs for an API instrument for law enforcement purposes (in EUR million)

	Airline industry*		***Member States***		***eu-LISA***	
	One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
Option 2.2	75	20.35	0	0	*No additional costs*	
Option 3.2	no additional costs ***	n.a.	n.a	n.a.	n.a	n.a.

** Due to limited availability of data, the assumptions and calculations include costs for both scheduled and non-scheduled carriers; ** the costs incurred are already included in the estimates presented in the API data capture for border management purposes.*

The envisaged instrument on API data for law enforcement purposes would not regulate the further processing of API data by the Passenger Information Units. To ensure the necessity and proportionality of the data processing under the envisaged instrument, and more specifically as regards the collection and transmission of API data on intra-EU and domestic flights, the processing would not be systematic but rather be limited to selected flights. Air carriers would only collect API data on those intra-EU and domestic flights for which Member States request the transmission of PNR data based on a risk assessment. The processing of API data in this context would be subject to the limits and safeguards established in the PNR Directive, as interpreted by the CJEU in the *Ligue des droits humains* case in the light of the Charter. The interference with the right to the protection of personal data relating to the collection and transmission of API data for law enforcement purposes would be justified and remain limited to what is strictly necessary. As regards the subsequent processing of the data, the PNR Directive already provides the Passenger Information Units with a legal basis to process API data they receive.

The interference with the right to freedom of movement relating to the collection of API data for law enforcement purposes would be justified and remain limited to what is strictly necessary. In particular, in addition to following the same requirements and safeguards as spelled out by the CJEU in the *Ligue des droits humains* case for the collection of PNR data on intra-EU flights, passengers would have the possibility to provide their API data free of charge at the airport (at a check-in desk, at a self-service kiosk or during boarding) if they do not wish to provide the data using their smartphones during online check-in. The essence of the freedom to conduct a business would not be affected.

8.3. Application of the 'one in, one out' approach

As assessed in section 6 and Annex 3, extending the scope of API transmission on inbound and outbound flights, as well as on selected intra-EU and domestic flights would result in additional burden for the air industry. More specifically, this initiative would require the following administrative costs for airlines:

- Recurrent **costs for the transmission of API data** on inbound, outbound, selected intra-EU and domestic flights to competent authorities, competent

border authorities and Passenger Information Units in Member States (estimated at a total of EUR 25,40 million per year[100]). The transmission of the API data to the carrier interface and use of the API router would lower these costs to a total of **EUR 17,82** million per year[101].

- One-off costs to adapt IT systems for the transmission of API data, estimated at a total of **EUR 75 million**.
- One-off costs for the **capture of API data using automated means** is estimated at a total of **EUR 50 million**.

8.4.REFIT (Simplification and improved efficiency)

Per the Commission's Regulatory Fitness and Performance Programme (REFIT), all initiatives aimed at changing existing EU legislation should aim to simplify and deliver stated policy objectives more efficiently (i.e. by reducing unnecessary regulatory costs). However, the proposal stemming from the impact assessment will be a new legislation that will replace the current API Directive. It will be implemented by adopting two new instruments. While this initiative has not been subject to REFIT initiative, it will significantly reduce the overall burden on administrative costs for air carriers thanks to a reduced costs and communication infrastructure (i.e. the carrier interface and the router) for the transmission of API data.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The Commission would ensure that the necessary arrangements are in place to monitor the functioning of the measures proposed and evaluate them against the main policy objectives. The mandatory nature of the obligation to collect API data and its transmission to the API router (annex 7) would allow for a clearer view on both the transmission of API data by air carriers and the use of API data by Member States. This would support monitoring and evaluation activities: the API router would generate statistics at central level and would provide information on API data transmitted and used on the type of flights (inbound, outbound, intra-EU and domestic). This will support the monitoring of air carrier's compliance with their obligation to transmit API data, and result in a regular, complete and stable collection of data for the benefit of Member States and the Commission

For the **API instrument for Schengen external border management**, the statistics would include indicators to measure the compliance of air carriers of their obligation to send API data and indicators on the use of API data by competent border authorities. These indicators would be the following:

- Number of passengers for which API data is transmitted;
- Number of inbound extra-Schengen flights for which API data is transmitted;
- Number of API messages transmitted on time to competent national authorities;
- Completeness of API messages (e.g. API messages with complete identity data);
- Individual and aggregated sum of penalties imposed by Member States on air carriers for not respecting their obligations;

[100] Cumulated gross for policy options 1.1 and 2.2 as reported in *Table* 8 Gross and net yearly costs for airlines (EUR million)
[101] Cumulated net costs of options 1.1 and 2.2 as reported in Table 8 Gross and net yearly costs for airlines (EUR million)

- Number of confirmed matches against national, EU (Schengen Information System) and international databases (Interpol's Stolen and Lost Travel Documents).

Taken together, these indicators would provide a strong indication of the success of this initiative to strengthen the use of API data for external border management purposes.

The follow-up to matches in databases and information on the practical results of these matches (e.g. whether a person sought in the watchlists was refused entry or apprehended) would fall outside the scope of the statistics collected, however it could be included as a qualitative indicator of the success of the initiative, for the evaluation of the instrument. Likewise, the evaluation could also include assessing the impact of the use of API data on border processing time per category of passengers (EU citizen, third country nationals holding a visa and those exempted from a visa, etc).

The API instrument for **law enforcement** purposes would seek to enhance the effectiveness of the joint processing of API data and PNR data by the Passenger Information Units in a systematic manner. Therefore, the main indicator to measure its success would be the percentage of the so-called 'false positive' matches – i.e. cases where an automated match is not confirmed manually by an officer of the Passenger Information Unit – e.g. because the PNR data proved unreliable or inaccurate.

While the collection of these statistical indicators would fall under the scope of the statistics currently collected under the PNR Directive, the API router would support gathering detailed statistics on, for instance, the number and the categories of passengers, or the number of flights (extra-EU, intra-EU or domestic) for which API data is transmitted by airlines and collected by Passenger Information Units of the Member States for law enforcement purposes.

The implementation of these instruments would be done through separate reports that will be presented to the European Parliament and the Council. To do so, the Commission would take into account the information provided by Member States and any other relevant information related to the implementation of the two instruments. The report on the API instrument for Schengen external border management would take place four years after the commencement of operations, meaning once carriers start transmitting data to the API router. Such report could be accompanied by a specific stakeholder consultation to assess the success of the instruments, particularly the effects of the transmission of API data to the router from the viewpoint of the industry and competent national authorities receiving API data. The report would also report on any direct or indirect impact on fundamental rights. It would examine results achieved against objectives and assess the continuing validity of the underlying rationale and any implications for future options. The effects of the second instrument on the use of API data for law enforcement purposes would better fit within the framework of an evaluation or report on the implementation of the PNR Directive.

Annex 1: Procedural information

1. LEAD DG, DECIDE PLANNING

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME) for the preparation of the initiative and the work on the evaluation and impact assessment. The agenda planning reference is PLAN/2019/5452.

2. ORGANISATION AND TIMING

The inception impact assessment was published on 5 June 2020. Within this framework, the impact assessment were subsequently prepared. An Inter-Service Group for the preparation of this impact assessment was set up in May 2022 with the participation of the following Commission Directorates-General: Secretariat-General (SG); Legal Service (LS); Justice and Consumers (JUST); Mobility and Transport (MOVE). The Inter-Service Group met twice (8 June 2022 and 6 July 2022), discussing (1) the envisaged policy options and the outline for the impact assessment, and (2) the draft impact assessment.

3. CONSULTATION OF THE RSB

On 31 August 2022, the Directorate-General for Migration and Home Affairs submitted the present impact assessment report to the Regulatory Scrutiny Board. Following a meeting on 28 September 2022, the Regulatory Scrutiny Board issued a positive opinion on the report on 30 September 2022.

4. EVIDENCE, SOURCES AND QUALITY

This impact assessment is notably based on the stakeholder consultation (see *Annex 2*).

The Commission applied a variety of methods and forms of consultation, ranging from consultation on the **Inception Impact Assessment**, which sought views from all interested parties, to targeted stakeholders' consultation by way of surveys, experts' interviews and targeted thematic technical workshops, including practitioners at national level.

In this context, the Commission also took into account the findings of the "*Study supporting an impact assessment: Potential effects of different possible measures on advance passenger information*"[102], which was commissioned by DG HOME.

[102] https://op.europa.eu/en/publication-detail/-/publication/dc1bdb12-2a3c-11ec-bd8e-01aa75ed71a1.

Annex 2: Stakeholder consultation

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

1. CONSULTATION STRATEGY

The objective of the consultation activities was to gather data and stakeholders' views in the context of preparations of the evaluation and revision of the API Directive, including for the purpose of this impact assessment.

The consultation activities aimed at collecting views on the issues at stake and suggested EU involvement, as well as opinions, ideas and concerns about possible solutions and impacts. The activities also sought to collect objective data, information, and evidence on how the proposed solutions would impact on the current landscape (cost benefit analysis).

The consultation sought to identify the relevant stakeholder groups and which consultation methods were best suited for the different audiences in order to receive relevant input to enable an evidence-based preparation of a possible legal proposal streamlining and improving the transfer and use of API data.

Commission services (DG HOME) also set up a **dedicated webpage for the initiative** that serves as the major information tool on the progress in the preparation of the proposal.[103]

The consultation process included:

- Consultations on the **Inception Impact Assessment**;
- Consultations for the purposes of this impact assessment: taking into account the technicalities and specificities of the subject, the Commission services organised **targeted thematic stakeholder workshops** that focused on subject matter experts, including practitioners at national level;
- Commission services also took into account the findings of the external study in support of this impact assessment (*Study supporting an impact assessment: Potential effects of different possible measures on advance passenger information*), which was commissioned by DG HOME and developed by an external contractor.

The consultation activities carried out for this impact assessment built on the data collected as part of the **evaluation of the API Directive** complemented in September 2020 and **review of the PNR Directive**, also completed in 2020, to minimise the administrative burden of already consulted stakeholders.

1.1. Mapping of stakeholders

When preparing the initiative, Commission services carried out an initial mapping of stakeholders that might be concerned by the revision of the Directive. These included:

[103] https://home-affairs.ec.europa.eu/whats-new/evaluations-and-impact-assessments/border-and-law-enforcement-advance-passenger-information-api-revised-rules_en;

- European Union Agencies (eu-LISA, European Border and Coast Guard Agency, Eurpol, European Union Agency for Fundamental Rights);
- European Commission internal stakeholders from different Directorates-General and services (DG for Mobility and Transport, DG Justice and Consumers, DG for Taxation and Customs Union);
- International organisations (International Civil Aviation Organisation, World Customs Orgnaisation, International Maritime Organisation) ;
- Competent authorities at Member State level, which included both authorities responsible for border management and Passenger Information Units;
- International and European industry organisations in the air, maritime, rail and road transport sectors;
- airlines, land and maritime carriers and private IT solutions providers;

The revision of the API Directive may also have an impact on the general public (particularly on passengers), therefore the mapping of stakeholders also included representatives of the European Passengers' Association and civil society organisations (Access Now).

The aforementioned diversity of perspectives proved valuable in supporting the Commission to ensure that its proposal address the needs, and took account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary data, facts and views on the effectiveness, efficiency and EU added value of the initiative.

1.2. Methods and forms of consultation

Considering the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

The consultation activities were launched with the publication of the **Inception Impact Assessment**, which lasted from 5 June 2020 to 14 August 2020.

As regards the **general public**, namely passengers and civil society organistions, a **public consultation** was carried out end of 2019 in the framework of the evaluation of the current API Directive.[104] Owing to the very technical nature of the subject (dealing with the type of data elements and capture methods), the public consultation triggered limited replies from the general public and it was decided not to use this method to integrate the views of the passengers in the impact assessment. The same result can be achieved by involving the passengers' associations via the targeted consultations which are more likely to be acquainted with the technicalities of the functioning of an API system. As the initiative concerns the use of passenger data, consultations reached out to relevant organisations to gather their views. This impact assessment also contains a thorough fundamental rights assessment of the measures proposed.

[104] Evaluation of the API Directive, SWD(2020)174, p. 61 onwards.

Targeted consultation activities were aimed to build on the consultation activities that took place in the course of a study to support this impact assessment commissioned by DG HOME and developed by an external contractor based on desk research and following stakeholder consultation methods:

- Two surveys for the API and PNR community (border management authorities, law enforcement authorities and passenger information units);
- A survey for industry stakeholders (air, maritime, railway and road transport sectors).
- Telephone or face to face interviews or group interviews with EU institutions and agencies, selected national authorities in Member States, International and European industry associations; international organisations, passenger associations and NGOs, technological solutions providers.

These stakeholder consultations by way of the external study were carried out between September 2021 and March 2022. An overview of the consultation methods used to reach out to and gather responses from the various stakeholder groups are presented in Table 1.

Table 1: Overview of stakeholders consultation

Stakeholder type	**Organisations**	**Mode of consultation**
EU institutions and agencies		
European Commission	Policy units within: DG HOME, DG MOVE, DG JUST, DG TAXUD	Interviews
European Agencies	Policy units within: EBCGA, eu-LISA, Europol and FRA	Interviews
National authorities in Member States		
Border management and law enforcement authorities	API units, Passenger Information Unit	Survey Interviews
Transport sector		
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) European Passenger Transport Operators (EPTO) Community of European Railway and Infrastructure Companies (CER) Alliance of Rail New Entrants (ALLRAIL) International Association of Public Transport (UITP) European Business Aviation Association (EBAA) European Community Shipowners' Associations Airports Council International Europe	Survey Interviews
Individual carriers	Danish Shipping (DK) Assarmatori (IT) Svensk Sjöfart (SE) Transportföretagen (SE)	Interviews
Technological solutions providers	Société Internationale de Télécommunications Aéronautiques (SITA) Amadeus Travelport Sabre	Interviews
International organisations		

	International Civil Society Organisation World Customs Organisation Organisation for the Security and Cooperation in Europe International Maritime Ooganisation	Interviews
Passenger associations and NGOs		
	European Passengers' Federation (EPF) Access Now	Interviews

2. CONSULTATION ACTIVITIES

2.1. The Inception Impact Assessment

The inception impact assessment received a total of seven answers from various types of stakeholders: 1 public authority , 2 airline industry associations , 1 airline and 1 airline service provider , 2 non-governmental organisations , and 1 railway industry association. .

All the responses are fully available online.[105]

The feedback received concerned the following subjects: extension of the scope of the future API Directive, data quality and sanctions, relation of API and PNR data, and protection of personal data.

Scope of API Directive: Airline industry associations highlighted that an extension in the scope of the collection of API data should assess: the impact on the passenger experience and speed of border control flows at airports; impact on the industry, from a facilitation, operational and cost perspectives, with special emphasis on intra-EU and outbound extra-EU flights. The assessment should also consider pre-existing measures in place at EU level in border management, such as the Entry Exit System and the European Travel Information and Authorisation System, which may overlap with a possible extension of new API legislation, resulting in an ineffective patchwork of requirements.

Regarding the **type of flights** for which API data should be collected and processed, feedback from an airline and and an NGO suggested limiting the use of API data to inbound flights from a well-defined set of third countries, to improve border controls and combat illegal migration as currently provided by the API Directive. Other feedback from air carrier industry expressed support for the widening of the scope of API legislation to other type of flights, i.e. on intra-EU flights where the extension of the collection should be balanced with the free movement enjoyed with the EU . Air carrier industry representatives also observed that technology solutions exist to support the submission of API data for non-scheduled air carriers as well, such as business aviation, which remain a gap and a risk in terms of border control evasion, criminality and smuggling.

Data quality: As regards further impacts on the industry as a result of the initiative, Easyjet flagged the need to mitigate the potential negative impact resulting from the costs for implementing technical solutions to collect API data as well as for the sanctions for untimely or incorrect transmission of API data. Air carrier industry representatives further

[105] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12434-Border-law-enforcement-advance-air-passenger-information-API-revised-rules_en.

pointed out that any fines for the failure to transfer API data should be imposed as a last resort, for example when there is a failure to cooperate.

Interaction with the PNR Directive. The feedback of Air carrier industry and a national authority emphasised that any future measure regulating the API framework should provide a higher level of harmonisation across Member States, especially in relation to the collection and processing of PNR data. Easyjet stressed that this revision should be an opportunity to clarify the differences between API and PNR data, address the gaps between the application of API legislation and the PNR Directive. According to Easyjet, such measure would be necessary due to the confusion from the requesting national authorities regarding the difference between PNR and API data, and the different type of obligations imposed on air carriers by the two Directives.

Personal data protection. Two NGOs, emphasised that the future API framework should be in line with EU data protection requirements as set out in the GDPR. Accordingly, this framework should foresee an exhaustive and closed list of API data fields – which would not leave space for extension at Member States' level. These organisations did not express support for the addition of the law enforcement purpose to a revised API framework as the main objective of such addition would serve mainly the objectives of the PNR Directive. Therefore, in their view, this issue should rather be addressed in the PNR Directive.

Extension of an API obligation to other modes of transport. A rail industry association expressed its concerns regarding the potential extension of API data collection to include other modes of transport. It highlighted in its feedback the differences between the railway transport sector and the aviation sector: European railways do not collect information on passengers as requested by the API Directive. The lack of obligation for a nominative ticket and lack of check-in obligation for rail transport and the possibility for the passenger to interchange, using the services of different carriers and on the basis of different tickets and the possibility to discontinue a journey by a passenger at any time, without obligation to inform the carrier, make a collection of API data challenging for the sector without brining major changes to how the railway business operates.

In contrast, a representative of an air carrier industry was in favour to include other modes of transport, and collect traveller information for all border crossings, including land and maritime borders, as it would represent a significant step in closing security gaps. A national authority was also supporting an extension to other modes of transport in view of developing harmonised criteria across the Member States on the collection and use of data, and therefore increase buy-in from carriers.

2.2. Targeted stakeholder consultations

An **external study**[106] supporting the elaboration of this impact assessment was contracted by Commission services. The objective of the study was to consider some specific aspects of a future instrument on API, assessing possible measures that would ensure effective processing of API data for border management and law enforcement purposes (e.g. scope of API data data fields, on the scope of application of API-related obligations on air carriers' flights, extension of the scope ot other modes of transport, measures to improve API data quality).

[106] See results of the study: Final report, analysis of survey results and interviews.

Building on the information collected for the 2020 evaluation of the API Directive, additional stakeholder consultations, such as surveys and targeted interviews with a wide range of stakeholders, were carried out from September 2020 to March 2021. Data collection consisted of:

- Extensive interviews with stakeholders at EU level, industry representatives and national authorities. In total, 28 interviews were carried out: 22 interviews with 24 stakeholders at EU or international level and six with national authorities from 4 Member States.
- One survey targeted industry associations and carriers of the three modes of transport, while two other surveys targeted national authorities (border management and law enforcement authorities). The industry survey received 27 responses – 20 air carriers, four land carriers and three maritime industry representatives. The air carriers who responded to the industry survey included some of the largest carriers in Europe and globally, including national carriers, and low-cost carriers, primarily operating inbound extra-EU flights and not EU-based.
- Two surveys targeted border management authorities and law enforcement authorities and were disseminated with the support of the Council Working Groups (Frontiers and IXIM). Responses were received from 20 border management authorities and 15 law enforcement authorities.

In addition to these preparatory consultations, in the context of the preparation of the initiative and the impact assessment, the Commission services organised additional three technical workshops which were held on 25 January 2022, 15 February 2022, 21 April 2022, respectively, to which representatives of the Member States, of the Schengen Associated Countries as well as EU agencies and the General Secretariat of the Council were invited. The workshops aimed at bringing together end-users for an exchange of views on the options, which were being envisaged and assessed to strengthen the future API framework, from a technical perspective. In addition to these three workshops, a consultation with the air industry representatives was also organised in March 2022.

2.1.1. Technical workshop 2: use of API data for fighting crime and terrorism (15 February 2022)

This workshop discussed the strengthening of API for border control purposes, with the possible introduction of a central router, and the options to collect better quality API data. Participants to the workshop included national experts from all Member States and Schengen Associated Countries, Europol, Frontex, eu-LISA and the General Secreterariat of the Council.

A general consensus emerged from the workshop for the future revision of the API Directive to reinforce the capacity of national authorities to perform checks prior to departure and for the revision to introduce future-proof changes. Support was expressed for a mandatory collection of API data on all in-bound extra-Schengen/EU flights, which will likely also induce costs for national authorities to upgrade their systems where relevant. A consensus on the extension of the retention of the data period to 48h also emerged from the exchanges. For reasons of data quality, there was also an overall support for increasing the automatic means to capture API data (Machine Readable Zone of the travel document).

2.1.2. Technical workshop 2: use of API data for fighting crime and terrorism (15 February 2022)

This second workshop focused the possibility to use API data for fighting crime, notably on the collection and use of API data on intra-EU flights. Participants to the workshop included national experts from all Member States and Schengen Associated Countries, Europol, Frontex, and the General Secreterariat of the Council.

It emerged clearly from the discussions that API data is mostly useful and yields best results when combined with PNR data. The combined use of API and PNR data help complete the travel history of a passenger and complete the risk profiling, particularly in foreign terrorism fighting cases. API data is better suited for comparison with certain databases where searches can be done using name-surname-date of birth. The extension of the collection of API data to intra-EU flights emerged as a general consensus from the discussions.

2.1.3. Technical workshop 3: API data collection from other modes of transport and use for health purposes (Thursday 21 April 2022)

This third workshop focused the possibility to collect API data from other transport modes abd use of API data for health purposes. Participants to the workshop included national experts from all Member States and Schengen Associated Countries, Europol, Frontex, and the General Secreterariat of the Council.

The discussions on the extension of API requirements to other modes of transport did not reach a clear consensus. The maritime transport sector is already under the obligation to transmit passenger and crew data to border (port) authorities 24 hours prior to arrival through the national maritime single window. No clear consensus on the necessity for an additional API obligations on maritime transport operators emerged from the discussions. Some Member States (e.g. Belgium, Estonia, Finland, France) develop at national level projects to collect passenger data from rail and international coach operators. The discussions showed that there could be a benefit of developing EU-level requirements to ensure better compliance by the transport industry concerned (avoid facing different requirements per Member State). Overall, the discussions showed a limited interest in applying a future API instrument to other modes of transport.

The discussion on the use of API data for health purposes was equally inconclusive due to API data not containing the contact details of a passenger (e.g. email or telephone number), as this type of information falls within the remit of the PNR Directive. In turn PNR data can only be processed for the purposes included in the Directive, namely to fight serious crime and terrorism.

2.1.4. Consultation of the air industry representatives (22 March 2022)

This consultation was aimed to gather the views of industry representatives in the context of the preparation of the impact assessment. Participants included associations (IATA, A4E, ERA, EBAA), air carriers (e.g. Lufthansa, KLM, Air France, Emirates) and service providers (Amadeus, SITA).

Participants highlighted the need for a single set of API data, as well as harmonisation on the timing of submission and number of submissions. Participants also flagged that collecting API data on intra-EU flights would have an important impact on how the industry operates flights between Member States, including the volume of data to be transferred to

national authorities. On improving API data quality and capture, and the possibility to use automated capture of the MRZ of the travel documents, air industry representatives flagged that many travellers do not use smartphones or apps for the check-in. The option to mandate automated means to collect API data would imply strong investment for carriers. Participants insisted on the need for flexibility on the modes to capture API data and the ways to collect personal data from passengers.

Annex 3: Who is affected and how?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

The initiative primarily benefits individuals and society at large, by improving security at the borders and internal security.

The practical implications are given by stakeholder group. The quantification of benefits is however difficult to undertake, the main reason being that attribution effects cannot be fully ascertained. API systems are widely and commonly used in conjunction with other border management and law enforcement tools, making it difficult to isolate their impacts on wider societal outcomes, such as national and EU security.

The practical implications are given by stakeholder group.

1.1. Citizens/Passengers

By facilitating the entry at Schengen borders, low-risk passengers would benefit from this initiative that would speed up their clearance. Detecting suspicious individuals prior to arrival would improve passenger experience as suspicious individuals would be discreetly diverted: passengers requiring more in-depth checks would be separated from other passengers, reallocated to separate lanes without the other passengers queuing and waiting.

A clear impact of the initiative on the waiting and clearance times at the border was difficult to estimate due to other factors than the use of API data such as the overall sustained increase in passenger traffic. The introduction of systematic verification and authentication of the travel-document of all persons crossing the external Schengen borders, the systematic checks in SIS, Interpol's Stolen and Lost Travel Documents (SLTD), and national systems, as per Regulation 2017/458,[107] may have also affected the average processing and waiting time for passengers.[108]

With the automated collection of API data, passengers would benefit from a faster check-in as the MRZ data would be automatically and securely collected from the travel document or identity card. Compared to manually transcribing information during check-in, the automated extraction of data would mean fewer error entries (e.g. which could result for example from the auto-fill forms functionalities or other clerical errors when manually inserting data). In contrast to current practices of certain airlines[109] whereby passengers need to pay a fee when choosing to check-in at the airport counter, this initiative would bring clarity that such practices would no longer be possible.

This initiative would also affect passengers by the processing of API data in terms of its implications on their personal data and privacy. The 2020 API Directive evaluation and in particular the consultations with the European Passenger Federation which indicated that the implementation of API systems in Member States did not give rise to specific complaints specifically related to the API data collection and processing, likely due to the fact that API

[107] 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

[108] See European Commission, Report as regards the reinforcement of checks against relevant databases at external borders introduced with Regulation (EU) 2017/458 amending Regulation (EU) 2016/399, COM(2022) 302 final, 24.05.2022, p. 13.

[109] Certain low cost companies (e.g. Wizzair, Ryanair, airBaltics) charge an airport check-in fee to passengers who did not check-in online or via an mobile app.

data is not perceived as sensitive information since API data concerns data included in travel documents and boarding passes, which are in any event shown to border authorities at border checks.[110]

To ensure that the rights of passengers are respected where the joint processing of API and PNR data would be possible for law enforcement purposes, the measures put forward in this initiative would follow the requirements and safeguards of the PNR Directive and recent case law of the Court of Justice.

1.2. Air carriers/businesses

Carriers would benefit from a greater clarity in the level of harmonisation of requirements in the data collection and transmission across the EU. As this initiative would provide a higher level of harmonisation across the Member States regarding the requirements for the collection and transmission of API data, in line with international standards and recommendations, it would increase compliance by the industry.

Airlines would benefit from a standardisation of data fields which would go hand in hand with the standardisation of the data transmission requirements. More specifically, API data would be transmitted only once to the carrier interface and its API router component. This would replace the current situation whereby the same API data collected on the same passenger on the same flight is sent to multiple authorities (to Passenger Information Units, to competent border management authorities). This is particularly relevant and would bring economies of scale on intra-EU flights. Indeed, the collection and transmission of API data on intra-EU flights would represent a novelty and additional costs for those carriers operating flights between Member States and domestic flights and that were only required to transmit PNR data.

Air industry would benefit from the capability of the API router to 'filter' the data and transmit it to competent authorities who would have direct access to the data instead of the individual system of the airline which may result in mistakes and loopholes. Therefore, a standardisation of the the data collection and transmission requirements is more efficient in ensuring correctness of the data and would significantly decrease the exposure to sanctions by Member States.

The collection of API data on intra-EU and domestic flights would also impact the check-in processes of airlines as, at present, the step of collecting data from identity cards or travel documents is not foreseen on these flights. The increasing use of online check-ins was a means for the air industry to bring down the costs associated with the check-in. The measures proposed aim to strike a balance between these costs to collect API data from passengers while also ensuring high quality of the data transmitted, containing as few errors as possible and less exposition to sanctions from national authorities.

The scope of the initiative would also extend to other types of carriers, operating non-scheduled flights such as business aviation and charter flights. At present, most of these operators do not have automated systems to collect API data and therefore do not use service providers to transmit data. They rely on the logistics and infrastructure already available – either in airports or of other bigger airlines. For this category of air carriers, a

[110] SWD(2020)174, p. 30

more cost-efficient solution to setting up full IT systems for the collection and transmission of API data consists of submitting API data through a web-portal. This solution is technically viable and currently deployed by eu-LISA to connect air carriers to the carrier interface as part of the implementation of the ETIAS and EES systems (see annex 7). This would be adaopted to their business model and a more cost efficient solution for air carriers operating non-scheduled flights such as business aviation that often do not carry as many passengers as on regular/scheduled flights.

1.3. National authorities in Member States

1.3.1. Border management authorities

The processing of API data on inbound extra-Schengen flights would mostly benefit the competent border management authorities of Member States. A stronger API instrument in this context would increase these 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. A higher quality of API data would also improve the use of API data to pre-check databases such as the Schengen Information Systems, other databases or watchlists of known suspects.

1.3.2. Passenger Information Units (PIUs) as set up by the PNR Directive

Better passenger data and verified identification data/travel document data would support Passenger Information Units in their analysis of passenger data, for example confirming that a person is on board, thus reducing the time necessary to identify relevant passengers. Better quality data would contribute to reducing false positives in the processing of passenger data.

1.4. eu-LISA

eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, will only be involved in building the central EU-level components to streamline the transmission of API data by airlines to one single point at EU-level, namely the API router added to the carrier interface. The carrier interface is being developed and will be implemented as part of the implementation of ETIAS and EES Regulations. The initiative to revise the API Directive would therefore build upon existing capabilities set up at EU level, with additional implications for the Agency consisting of the development of the API router component attached to the carrier interface.

eu-LISA would start working on this component as of 2028, to then effectively connecting air carriers by 2029.

2. SUMMARY OF COSTS AND BENEFITS

The overview of costs of the preferred policy options is indicated below.

I. Overview of costs – Preferred option (EUR million, recurrent per year)									
		Air carriers		**Member States**		**Citizens/Consumers**		**eu-LISA**	
		One-off	**Recurrent**	**One-off**	**Recurrent**[111]	**One-off**	**Recurrent**	**One-off**	**Recurrent**
Option 1.1. API data on all extra-Schengen inbound flights	Direct administrative costs	0	2,95	13.5	0	0	0	34	1.4
Option 2.2 API data on all extra-EU, intra-EU and domestic flights	Direct administrative costs	75	22,45	0	0	0	0	0	
Option 3.2. API data collection by automated means only	Direct administrative costs	50	0	0	0	0	0	0	0
Costs related to the 'one in, one out' approach									
Total	Administrative costs (for offsetting)	125	25,40			0	0		

[111] Referred to as gross costs in Table 8 Gross and net yearly costs for airlines (EUR million)

All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified and these are therefore not quantified. These are all provisional estimates that would need to be confirmed. As a result the confidence margin of cost estimates cannot be better than 20-25% at this early stage in a project. What is stable is how the costs of the various measures compare with each other.

As can be concluded from the above table, in conjunction with the table hereunder:

- For airlines, the one-off total costs amount to EUR 125 million and recurrent **net** costs to EUR 36,32 million *per annum*.
- For Member States authorities, the one-off total costs amount to EUR 13,5 million, with no significant recurrent costs.
- For eu-LISA, the one-off total costs amount to EUR 34 million and recurrent costs to EUR 1.4 million *per annum*.

II. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
N/A		
Indirect benefits		
Reduced fines due to improvement of data quality	Up to EUR 80m recurrent	Airlines
Administrative cost savings related to the 'one in, one out' approach*		
Reduced costs of transmitting inbound API data due to the router	€5,49m recurrent	Airlines
Reduced costs of transmitting outbound API data due to the router	€2,11m recurrent	Airlines
Reduced costs of transmitting intra-EU and domestic API data due to the router	€0,00m recurrent	Airlines

All benefits are reduced implementation costs and are based on very cautious estimates, which for instance do not consider economies of scale in the context of the transmission of API data. The benefits include reduced costs for the airlines due to the introduction of the API router, which halves the transmission volume for each category of API data (except for domestic flights).

As can be concluded from the above table, the recurrent benefits for the airline industry following the implementation of the carrier interfance and the API router amounts to EUR 7,6 million per *annum*.

Moreover, the mandatory collection of API data by automated means would incur in a reduction of fines (estimated at potentially up to EUR 80 million per year). Which means that the one-off costs invested by the airline industry for improving data quality would partly be recouped by the fact that no more financial sanctions would be imposed.

The most important benefit — the contribution to fighting crime and terrorism — is not monetized either in the above calculation.

Annex 4: Analytical methods – calculating the costs and savings

This annex provides a summary of the methodological approach taken to estimate the financial costs of the various policy options presented in this impact assessment.

The underlying assumptions are based on the data-collection exercise conducted during the recent evaluation of the API Directive and during the external study that supports this Impact Assessment.[112]

It should be noted that the data-collection, particularly of quantitative evidence, was challenging. Building on the information received during the evaluation, detailed questionnaires were sent to Member States authorities in October 2020 to provide (and complete) evidence on elements such as share of API data collected on flights, number of hits obtained when verifying API data against databases, as well as evidence on costs (one-off, recurrent costs,) incurred for the establishment of API systems and other administrative costs. While most (20) Member States replied, only three Member States sent all the data asked, with remaining Member States sending only partial data.

Consulted via survey and interviews, air carriers were also sollicited to provide quantitative evidence necessary to assess the impacts of possible options (e.g. extending transmission to all extra-Schengen/EU flights, intra-EU flights, use of automated means to collect data, etc). This impact assessment integrates data that was shared by commercial air carriers (e.g. average cost for setting up a system to collect data). Little to no quantitative evidence was obtained from carriers operating non-scheduled flights such as business aviation.

Hence the analysis on the impacts of the options on national authorities and aviation sector rests on a number of assumptions and average estimates presented in the sections below.

1. INTRODUCTION

The capturing, transmission and processing of API data generates financial, human-resource and 'time spent' costs on the various entities that are involved:

- Passengers
- Airlines
- Member States' border-management authorities
- Member States' law-enforcement authorities
- Member States' and EU service providers

The following sections present the cost-elements (where available) as background to the calculations of the economic impactsost elements of the various options explored in thise Impact Assessment.

[112] European Commission, Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 8 September 2020, SWD(2020) 174; European Commission, Directorate-General for Migration and Home Affairs, External Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, 2020; Study supporting an impact assessment: Potential effects of different possible measures on advance passenger information (final report and annexes).

2. PASSENGERS

For passengers the main cost-element is obviously the price of an airline ticket. Any additional burden imposed on an airline will ultimately be forwarded as a price-increase on the ticket. This is also the case for increases in fuel costs, airport charges, landing-rights, Eurocontrol surcharges, etc.

There are no direct cost-elements of the proposed initiative for the passenger other than those forwarded by the airlines.

3. AIRLINES

Airlines tend to outsource the IT related passenger handling aspects to service providers so they can focus on their core-business which is flying. Reservations are thus handled by globally operating companies like Amadeus, Travelport and Sabre. The entire logistics around passengers boarding to a plane, reserving the plane's take-off and landing slots and the handling of luggage, are performed by Departure Control Systems (DCS) that are also often outsourced to major companies like SITA, Amadeus and iPort DCS.

Where a public authority obliges an airline to provide API data (or PNR data), to add/modify the content of API data, to modify the timing of the transmission or to modify the methods of capturing the identity data from the passenger, this will ultimately be performed by service providers of the airline, inducing a cost for the airline which it will offset on the ticket-price.

Table 1: Number of air passengers carried in 2019 (EU-27)

	Inbound Extra-EU	***Outbound Extra-EU***	***Intra EU***	***Domestic***	***Total***
Number of passengers[113]	259,686,015	259,151,163	335,867,750	160,590,869	1,015,295,797
Share of passengers for which API data is curently collected (estimates)	65%	25%	0%	0%	
Number of passengers for which API data is currently collected	168.795.910	64.787.791	0	0	233.583.701
Number of passengers from which data is not currently collected	90.890.105	194.363.372	335.867.750	160.590.869	781.712.097

[113] Eurostat 2019 (avia_paoc) and external Study supporting an impact assessment: Potential effects of different possible measures on advance passenger information.

When assessing the financial costs of this initiative for the airline industry, a first cost-element relates to the possible **modifications to be made to the airline's IT systems** due to changes of the required API data elements or the timing or the number of transmissions. These would require changes to the Departure Control System (DCS) whose one-off cost are estimated, at a maximum, at EUR 500.000 per airline.[114]

A second cost-element for airlines relates to the way passenger identity **data are captured**. In line with best practices and global guidelines such data needs to be taken from the Machine Readable Zone (MRZ) of the travel document. The correct way to capture an MRZ is to perform an **Optical Character Recognition (OCR)** where a 'machine' scans the entirety of the information. This OCR technology is well established and widely used. The initiative would make this, under option 3.2, the compulsory mode of data collection, thereby inducing costs on airlines that do not have this in operation today. The estimated one-off costs for airlines to include this capability – in case they do use it already – in their online check-in applications (web-based or smartphone app-based) are **EUR 200.000**, based on estimates received from air industry.

The third, recurrent, cost-element of providing API-data is the '**transmission cost**' which encompasses processing, formatting, sending and verification of API data. The commercial contracts regulating the costs per reservation or per processing of an API (or PNR) message vary greatly. Airlines and service providers were not in the position to divulge these actual detailed costs, The calculation of the transmission costs per API message used in this annex is therefore an **estimate** based on average prices shared by a principal service provider of the air-industry:

- One API message contains 250 characters;
- The transmission of 1 million characters costs an average of EUR 130.
- Therefore, transmission costs are estimated on average at EUR 0,0325 per API message.

For the calculation of transmission costs, it is therefore assumed that for every message transferred to a border-management authority and for every message transferred to a PIU, an airline will pay on average **EUR 3,25 cents**. The cost elements above can be used to estimate an overall 'industry cost' for the following options:

- **Inbound-API Costs**

Since all airlines flying into the Schengen-area are currently sending API data, no changes or upgrades to the airlines IT systems are required.

Regarding transmission costs, as a result of this initiative some 91 million more API messages will be generated for inbound flights (today, around 65% of the 260 million incoming passengers generate the transfer of an API message; under options 1.1 and/or 2.1 of the initiative this will be 100%).

Total transmission costs: 90,89 million x 3,25 cents = **EUR 2,95 million.**

[114] Estimates provided by air industry associations for the external study supporting this impact assessment (December 2020).

- **Outbound-API Costs**

Since the majority of airlines flying out of the Schengen-are are currently required to provide API data to third countries, it is assumed that no system modifications will be required.

As for transmission costs, the initiative would result in some 194 million more API messages being generated for outbound flights (today, around 25% of the 260 million outgoing passengers generate the transfer of an API message; under options 1.2/2.1 of the initiative this will be 100%).

Total transmission costs: 194,36 million x 3,25 cents = **EUR 6,32 million**.

- **Intra-EU and domestic API Costs**

According to the airline associations, there are approximately 150 airlines (regular, business, charter) that operate flights exclusively within the EU. Today, these airlines do not process API data. The modifications to their Departure Control Systems will incur a one-time cost of 150 x EUR 500.000 (maximum), which constitutes a total investment costs of **EUR 75 million maximum**.

As for transmission costs, as a result of this initiative around 496 million additional API messages would be generated for intra-EU and domestic flights.

Total transmission costs of 495,46 million messages x 3,25 cents = **EUR 16,13 million.**

- **Good quality API Costs**

According to the airline's associations, there are approximately 1000 airlines operating flights to, from and/or within the EU. All these airlines (which include the 150 mentioned in the previous section) will need to ensure that their on-line check-in systems are equipped with Optical Character Recognition (OCR) technology to capture the API data from the MRZ of the travel document.

The avarage costs for installing an OCR capability is estimated at EUR 200.000 per airline (based on estimates provided by air industry during consultations), leading a maximum one-off cost for the sector of 1000 x EUR 200.000 = EUR 200 million.

Today, all manual check-in counters worldwide are equipped with terminals that allow “swiping” the MRZ of travel documents in order to capture the passenger's identity details as this is an ICAO requirement. In many airports, self-check-in kiosks have been installed that will also read the MRZ correctly by doing a full-page scan of the passport or an id-card. As a consequence, not all airlines will be impacted in the same way by the obligation to invest in OCR technology.

Not all airlines will therefore be affected in the same way by the obligation to invest in OCR technology. Based on surveys conducted as part of the external study supporting this impact assessment and further consutlations with air industry associations,[115] it is estimated that out of 1000 airlines, at least 75% will not need to make investments to allow for the machine reading of MRZ data of travel documents. Hence the average costs to adapt their OCR capability leads to a maximum one-off cost for the sector of (1000 x EUR 200.000) x 25% = **EUR 50 million**.

- **One-off cost by policy option**

One-off overall costs for the implementation by airlines of the initiative depends from three different policy options:

- the first one, on the scope of the collection for the border authorities : 1.1 on outbound extra Schengen, or 1.2 on inbound and outbound extra Schengen flights
- The second one on the scope of the collection for the PIUs : 2.1 on all extra EU, or 2.2 on all extra, intra and domestic EU flights. In either case, From that choice depends the number of DCS to be updated.
- the third one, on the means to collect API data : 3.1 for manual collection or 3.2 for automated collection. From that choice will depend the number of airlines concerned by deploying an automated process for collecting travel data.

Table 6 One off cost for one set of policy options

					3.1	***3.2***
Policy option	Number of airlines concerned	DCS to be upgraded	Cost of DCS upgrade (EUR million)	Cost of OCR (EUR million)		
1.1	850	0	0	170	**0**	**170**
1.2	850	0	0	170	**0**	**170**
2.1	850	0	0	170	**0**	**170**
2.2	1000	150	75	200	**75**	**275**

- **Yearly costs by policy option**

Costs are directly proportional to the number of messages API messages entailed by this initiative. Net costs for airlines take into account, on one side the *additional messages* not yet already sent on the basis of the existing regulation, and on the other side the *spared messages* that are actually sent but need not to be anymore. The volume on, respectively, *additional messages* and *spared messages*, depend on the policy option chosen on the scope of collection (see above One-off cost by policy option)

A first part of the *additional messages* will be transmitted to the router for border management purposes, e.g. on the basis of either policy option 1.1 or 1.2. A second part of

[115] https://op.europa.eu/en/publication-detail/-/publication/dc1bdb12-2a3c-11ec-bd8e-01aa75ed71a1/language-en.

the additional messages will be transmitted for law enforcement purposes ; those will actually depend on the ones already transmitted to the router for border management. Therefore, the cost of either policy option, 2.1 or 2.2, will depend on the choice made for border management, i.e. between policy option 1.1 and 1.2[116]. The overall "gross" transmission costs for the airlines are directly proportionate to the sum of the additional messages for border management (option 1.1 or 1.2) and of additional messages for law enforcement purposes (option 2.1 or 2.2.)

Spared messages are typically those that are currently sent twice by the airlines, for instance, once for the PIU, once for the border authorites, but which will be only sent once to the router, the latter taking care of forwarding it to the multiple destinees. Cost savings can be directly deduced from the volume of spared messages.

Table 7 Volume of additional and spared messages transmitted by airline, per policy option

		inbound extra	outbound extra	intra EU	domestic	**Additional messages**	**Spared messages**
1.1		90,890,105	n.a.	n.a.	n.a.	**90.890.105**	**168.795.910**
	2.1	0[117]	194.363.372	n.a.	n.a.	**194.363.372**	**64.787.791**
	2.2	0	194.363.372	335.867.750	160.590.869	**690.821.991**	**64.787.791**
1.2		90,890,105	194.363.372	n.a.	n.a.	**285.253.478**	**233.583.701**
	2.1	0	0	n.a.	n.a.	**0**	**0**
	2.2	0	0	335.867.750	160.590.869	**496.458.619**	**0**

Table 8 Gross and net yearly costs for airlines (EUR million)

		Additional messages(A)	***Spared messages(B)***	***Gross costs (G)=(A)*3,25ct***	***Costs Savings (S)=(B)*3,25ct***	***Net costs (N) = (G)-(S)***
1.1		90.890.105	168.795.910	**2.95**	5.49	**-2,53**
	2.1	194.363.372	64.787.791	**6,32**	2.11	**4,21**
	2.2	690.821.991	64.787.791	**22,45**	2.11	**20,35**
1.2		285.253.478	233.583.701	**9.27**	7.59	**1,68**
	2.1	0	0	**0,00**	0	**0**
	2.2	496.458.619	0	**16,13**	0	**16,13**

4. MEMBER STATES' BORDER-MANAGEMENT AUTHORITIES

Almost all **Member States** border-management authorities currently receive and process API data. Member States were however not able to provide insights into the actual current

[116] For instance, in the case where policy options 1.1 and 2.2 would be selected, the *additional API* messages to be transmitted would amount to 781.712.097 (the first part of 90.890.105 coming from policy option 1.1 would add up to the 690.821.991 coming from policy option 2.2)

[117] Already covered by transmission made for border management purposes

costs of this capability. Also, the costs for upgrading systems in order to process more data could not be provided. For that reason, when assessing investment costs for Member States the baseline used is the estimate of one Member State (that has not yet deployed its API system) that the set up and implementation of such system would cost EUR 5 million.[118]

Under this initiative, the volume of data that will need to be handled by Member States' authorities would substantially increase. Based on the EUR 5 million benchmark, it is assumed that on average 50% of this amount would be necessary to handle the additional data volumes, and to implement new processes where required.

Under option 1.1 (where the amount of API data would on average double, but the working process remain essentially the same) and additional investment of EUR 500.000 would (on average) be required per Member State.

For option 1.2 (where the amount of new data that would need to be handled is larger, and where many Member States would need to introduce new working flows) the required investment is on average estimated at EUR 2 million per country.

Costs of additional API handling for inbound flights (option 1.1): 27 Member States x EUR 0,5 million = **EUR 13,5 million**

Costs of additional API handling for outbound flights (option 1.2): 27 Member States x EUR 2 million = **EUR 54 million**

These financial implications are expected as of 2028, with impacts on the next Multiannual Financial Framework only.

5. MEMBER STATES' LAW ENFORCEMENT AUTHORITIES

All Passenger Information Units (PIUs) are currently receiving and processing API-data as a PNR-complement on inbound routes and on certain outbound routes. The API-data component is much smaller than the PNR-data component.

Under this initiative, the volume of data would slightly increase because of new data from outbound flights and selected intra-EU flights for which PNR data is collected.

The Member States were unable to estimate additional costs since the additional API-data are comparably small compared to the larger PNR set.

It is thus presumed that the additional costs for PIUs will be neglectable.

6. EU-LISA

Due to the European Travel Information and Authorisation System (ETIAS) Regulation, the Entry Exit System (EES) Regulation and the revised Visa Information System (VIS II) Regulation, carriers (air, sea, coach) will need to query these systems with passengers' travel document details when transporting them into the Schengen area.

[118] ee estimates included in the evaluation of the API Directive, SWD(2020) 174, p. 35.

For this purpose, eu-LISA has implemented a 'Carrier Interface' for these carriers to connect to. Under this initiative, the Carrier Interface would be re-used, to allow air-carriers to also deliver API-data for inbound, outbound, intra-EU and domestic flights.

Under this initiative, eu-LISA will install an 'API Router' behind this Carrier Interface, as a point of reception of API data sent by airlines, and as a point of distribution for onward transmission of this data to Member States' border authorities and/or PIU's, as appropriate.

As estimated by eu-LISA, the total cost for the Agency to increase the capacity of the Carrier Interface, to connect missing airlines, to implement an API Router and to host, operate and maintain this capability for 5 years is estimated at **EUR 40,4 million**.

7. SAVINGS

This initiative, and notably the implementation of the API router, is expected to generate important savings for the air industry and the Member States alike:

- **Savings for airlines**

The introduction of the API router will allow airlines to make important savings on their transmission costs.

For inbound flights the airlines will no longer need to send API data to the Member State's border authority and to the PIU separately, but only to the API router, once. Today, some 170 million API messages are sent twice. Under this initiative 260 million messages would be sent only once. With a price tag per message of 3,25 cents, this represents a total saving of **EUR 8,46 million**. In other words: whereas the number of passengers for which API data is transmitted would grow (from 65% to 100%), following the introduction of the API router the number of transmitted messages will actually be lower than today. Which means that the net financial effect on the airline industry will be positive.

Likewise, for outbound flights, with a current coverage of 25% of passengers for which API data is transmitted, the introduction of the API router represents again a financial saving of **EUR 8,46 million**.

Estimated number of API data messages transmitted (in millions)

	Current situation		**Future situation (without API router)**		**Future situation (with API router)**	
	passengers	*API messages*	*passengers*	*API messages*	*passengers*	*API messages*
Inbound flights	170m	340m	260m	520m	260m	260m
Outbound flights	65m	130m	260m	520m	260m	260m

For intra-EU flights, there would no longer be a need to send API messages to both the PIU in the country of departure and of destination. This saves 336 million messages, or **EUR 10,92 million.**

The implementation of the API router will also have a cost-saving impact on the overall IT budget of airlines. Instead of setting up and maintaining links with 27 Member States, they will only have to establish and maintain one single connection with the central API-router. The corresponding savings, albeit presumably important, could not be quantified.

A specific saving that needs to be mentioned is that airlines (under option 3.2) would have a far lower risk of being confronted with fines and sanctions. This amount is estimated at potentially up to **EUR 80 million** per year.

- **Savings for Member States**

As is the case for air carriers, the implementation of the API router will also have a cost-saving impact on Member States. Instead of setting up and maintaining links with all (potentially 1000) airlines, they will only have to establish and maintain one single connection with the central API-router. It however appeared not possible to quantify this (important) saving.

Annex 5: Clear and mandatory set of API data

1. INTERNATIONAL STANDARDS AND GUIDELINES ON API

Several international organisations called for the setting up of API systems and provided standards, recommendations and guidelines as to how to establish these systems, including which API data elements to reqest from airlines.

1.1. *Annex 9 (Facilitation) to the Convention of International Civil Aviation*

The Convention of International Civil Aviation, also known as the 'Chicago Convention', was signed in 1944 to promote international cooperation in air transport. The International Civil Aviation Organisation (ICAO), a specialised United Nations agency, was established in 1947 to support the cooperation among States parties to the Chicago Convention.

ICAO adopts **standards and recommended practices** (SARPs) which are contained in **Annexes to the Chicago Convention**. Standards are binding for Member States, all of which are parties to the Chicago Convention.

Annex 9 on 'Facilitation' is based on articles of the Chicago Convention requiring that the civil aviation complies with laws governing the inspection of aircraft, cargo and passengers by authorities concerned with customs, immigration, agriculture and public health. It deals with the facilitation of passengers and the steps taken to process each passenger on their arrival to and departure from a border.

Annex 9 has been revised periodically since its adoption in 1949, and is updated on the basis of discussions within two ICAO bodies, the Facilitation Panel and the Facilitation Division, both of which involve representatives of States party to the Chicago Convention and the air transportation industry.

In October 2017, **Annex 9 was updated to declare that each contract state shall establish an API system** (standard 9.5). As a result, the implementation of API systems became a UN standard in October 2017, and UN Member States must implement API systems to be compliant with Annex 9 of the Chicago Convention.

In addition, Annex 9 states that the API system shall be consistent with interntionally recognised standards for API (item 9.6). In this regard, Annex 9 states that the required API data should be limited only to data in the **Machine Readable Zone** (MRZ) (standard 9.8): "*when specifying the identifying information on passengers to be transmitted, Contracting States shall require only data elements that are available in machine readable form in travel documents conforming to the specifications contained in Doc 9303. All information required shall conform to specifications for UN/EDIFACT PAXLST messages found in the WCO/IATA/ICAO API Guidelines*."

However, the SARPs are **not directly applicable and require legal transposition into the national legal orders of the EU Member States**. This is done through EU legislation where the competence has been delegated to the EU. Secondly the SARPs usually require adaptation to make them fully operational when being transposed into EU law. This requires a rulemaking process with the involvement of the European Commission, and the co-legislators, the European Parliament and the Council. Relying only on ICAO SARPs is therefore not sufficient and does not guarantee uniformity of action within the EU.

1.2. *United Nations Security Council Resolutions (UNSCR)*

There have been repeated calls since 2014 by the UN Security Council to Member States to establish API (and PNR) systems in the fight against terrorism:

UN Security Council Resolution 2178(2014)[119] describes how UN Member States should cooperate in the fight against terrorism, including in the threat posed by foreign terrorist fighters returning or relocating, particularly from conflict zones, to their countries of origin or nationality, or to third countries.
The Resolution calls '*Member States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of in dividuals* [designated by UNSC ISIL and Al-Quaida Sanctions Committee]'.

UN Security Council Resolution 2309(2016)[120] describes how UN Member States should further work to combat terrorism particularly motivated by intolerance or violent extremism. It calls upon "*all States to work within ICAO to ensure that its international security standards are reviewed and adapted to effectively address the threat posed by terrorist targeting of civil aviation"* and further calls upon all States, as part of their efforts to prevent and counter terrorist threats to civil aviation […] to require advanced passenger information from airlines.

UN Security Council Resolution 2396(2017)[121] on threats to international peace and security caused by retirning foreign terrorist fighters, welcomed ICAO's decision to establish a standard under Annex 9 regarding the use of API systems by its Member States, also underlinng that many ICAO Member States are yet to implement this standard. It also required from UN Member States to require API data from airlines and to ensure that "*API is analysed by all relevant authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting, and investigating terrorist offenses and travel*."

UN Security Council Resolution 2482(2019)[122] on preventing and combating terrorism, including terrorism benefitting from transnational organized crime, called on UN Member States to "*implement obligations to collect and analyze Advance Passenger Information (API) and develop the ability to collect, process and analyse, in furtherance of International Civil Aviation Organization (ICAO) standards recommended practices, Passenger Name Record (PNR) data and to ensure PNR data is used by and shared with competent national authorities, with full respect for human rights and fundamental freedoms, which will help security officials make connections between individuals associated to organized crime, whether domestic or transnational, and terrorists, to stop terrorist travel and prosecute terrorism and organized crime, whether domestic or transnational, including by making use of capacity building programmes*."

---

[119] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/547/98/PDF/N1454798.pdf?OpenElement.
[120] https://undocs.org/S/RES/2309(2016).
[121] https://undocs.org/en/S/RES/2396(2017).
[122] http://unscr.com/en/resolutions/doc/2482.

OSCE Ministerial Council Decision 6/16 on Enhancing the use of Advance Passenger Information[123]

The Decision was adopted to support the implmenetation of the UN Security Council Resolutions, also aimed at the prevention of movement of terrorists, terrorist groups and foreign terrorist fighters through effective border controls. With this Decision, OSCE participating States committed to set up national API systems in accordance with the provisions contained in ICAO's Annex 9 to the Chicago Convention and aligned with the WCO/IATA/ICAO Guidelines on API.

WCO/IATA/ICAO API Guidelines[124]

First developed in 1993 by the World Customs Organisation (WCO) in cooperation with the International Air Transport Association (IATA), the API Guidelines were further developed with the participation of the ICAO. The three organisations published API Guidelines together since 2003 with regular updates, with the latest version dating to 2014.

WCO/ICAO/IATA API Guidelines are not standards as per ICAO requirements, their goal is to establish '*an agreed **best practice**, to which States and aircraft operators seeking to implement API systems can, to the greatest extent practical adhere*'.

These Guidelines contain a description of several items pertaining to the set up of API systems, such as a description of the type of API data (batch and interactive), API data capture and transmission.

Section 8 of the Guidelines refers to a **maximum set of API data** that can be requested by national authorities. The Guidelines further highlight that '*extending the required data element set beyond that limit would hinder carriers' operation and could potentially impact airport throughput and passenger capacity*" and that "*the API data must not exceed that given in this guideline*'[125].

API data is included in the **passenger list (PAXLST) message** used for the transmission of such data by the carriers. The standard for transmitting an API message is the UN/EDIFACT/PAXLST.[126]

The PAXLST message comprises **data relating to the flight and to each individual passenger and crew member**. In addition to passenger data, States have the option to request crew data.[127] WCO/IATA/ICAO **PAXLST implementation guidelines**, which is a

---

[123] https://www.osce.org/files/f/documents/4/f/288256.pdf.
[124] WCO/IATA/ICAO guidelines on API, 2014, available at: https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf.
[125] WCO/IATA/ICAO Implementation Guidelines, para 8.1.3.
[126] Annex 9 to the Chicago Convention, item 9.6: *The UN/EDIFACT PAXLST message is a standard electronic message developed specifically, as a subset of UN/EDIFACT, to handle passenger manifest (electronic) transmissions. UN/EDIFACT stands for "United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport." The rules comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data, and in particular that related to trade in goods and services between independent, computerized information systems. The WCO, IATA and ICAO have jointly agreed on the maximum set of API data that should be incorporated in the PAXLST message to be used for the transmission of such data by aircraft operators to the border control agencies in the destination or departure country.*
While the standard for transmitting an API message is the UN/EDIFACT/PAXLST, not all border management authorities are able to receive API messages in this format and may require transmission in another format (XML).
[127] Annex 9 to the Chicago Convention, item 9.6: *API involves the capture of a passenger's or crew member's biographic data and flight details by the aircraft operator prior to departure. This information is electronically transmitted to the border control agencies in the destination or departure country. Thus, passenger and/or crew details are received in advance of the departure or arrival of the flight*.

set of instructions on how the carriers must use the PAXLST format to transmit their data, make no distinction between passengers and crew members.[128] Passenger and crew (when requested) API data are generally transmitted as two separate messages to national authorities.

MANDATORY AND CLOSED SET OF API DATA

The WCO/ICAO/IATA API guidelines divides the set API data set into three categories (see table 1 below):

Core data elements, as found in the Machine Readable Zone (MRZ) of the official travel document;
Additional data as available in airline systems; and,
Additional data not normally found in airline systems and which must be collected by, or on behalf of, the airline.

In the **current API Directive**, the list of API data fields in Article 3(2) includes both passenger data and flight data (see Table 1 below). This list is not aligned with the list of recommended data as per the WCO/ICAO/IATA API Guidelines.

Based on the above and the external study supporting the preparation of this impact assessment, the **revised API instruments will include**, in addition to the current data fields listed in the Directive, **a mandatory and closed set of API data** to:

- Update the data relating to the **flight information** and include the scheduled departure time and scheduled arrival time.
- Align the data relating to the identification of the passenger and the travel document information with the **MRZ fields** (thus include the issuing State/organisation of the travel document, the expiration date of the travel document and gender).
- Collect, where such data is attributed to a passenger in the systems of the airline, data elements relating to **seating information and baggage information**, necessary for both border and customs control and the prevention and investigation of serious crime (e.g. drug trafficking, trafficking in human beings); on some non-scheduled flights, neither seating nor baggage information is generated.
- Collect, when available, the **passenger record locator number** to effectively support the joint processing of API and PNR data; a PNR locator number would only be generated where PNR data was also generated on a flight.
- Collect, when available, data elements relating to the **traveller's status** to enable receiving authorities to distinguish whether the data relates to a passenger, crew member or an in-transit traveller.

The inclusion of other data element would not be necessary and proportionate. For example those relating to visas or of primary residence, destination, etc, can either be found in other EU IT systems (e.g. Visa Information Systems) or will need to be collected manually by air carriers and therefore prone to errors.

[128] WCO/IATA/ICAO PAXLST Implementation Guidelines, version 6.0, 2016, available at: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/appendix-iia-paxlst-message-implementation-guide-2016.pdf

Set of API data in the current API Directive compared to international guidelines

API data elements as per WCO/ICAO/IATA Guidelines on API	MRZ[129]	API Directive	API data in the revised instruments
I. Data relating to the flight			
Flight identification		x	x
Scheduled departure date		x	x
Scheduled departure time			x
Scheduled arrival date		x	x
Scheduled arrival time			x
Last place/port of call of aircraft			
Place/port of aircraft initial arrival			
Subsequent place/port of call within the country			
Number of passengers		x	x
II. Data relating to each individual passenger (core data)			
Official travel document number (passport or other official travel document number)	x	x	x
Issuing state or organisation of the official travel document	x		x
Official travel document type	x	x	x
Expiration date of official travel document	x		x
Surname/given names	x	x	x
Nationality	x	x	x
Date of birth	x	x	x
Gender	x		x
III. Additional data as available in airline systems			
Seating information			x
Baggage information			x
Traveller's status (passenger, crew, in-transit)			x
Place/port of original embarkation			
Place/port of clearance			
Place/port of onward foreign destination			
Passenger Name Record Locator Number			x
IV. Additional data not normally found in airline systems and which must be collected by, or on behalf of the airline			
Visa number			
Issue date of the visa			
Place of issuance of the visa			
Other document used for travel			
Type of other document used for travel			
Primary residence			
Destination address			
Place of birth			

[129] https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf, p.17.

Annex 6: Complementarities and differences between Advance Passenger Information (API) and Passenger Name Records (PNR)

Passenger data is any information that has been collected and stored by an airline containing information on a passenger's identity or travel route, which is later used by public authorities for border management or law enforcement purposes. Passenger data can be divided into two main streams: Advance Passenger Information (API) and Passenger Name Records (PNR):

API is information on a 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.

PNR is a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each flight 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.

The table 1 below highlights the main features of API and PNR Directives.

Under the current API Directive, the main purpose of collecting API data is improving border control and combatting illegal migration. Using PNR data for this purposes is not allowed under the PNR Directive, which is exclusively a law enforcement tool requiring that data should only be used for prevention, detection, investigation and prosecution of terrorist offences and serious crime. API data can also be used for law enforcement purposes, but this is not regulated by the API Directive, who leaves this possibility to Member States to do so via national legislation.

The API Directive allows Member States to impose an obligation on carriers to collect API (the collection happens at the request of the Member State and for extra-EU inbound flights only) while the PNR Directive obliges carriers to transfer only the data that they have collected for their own commercial purposes, without requiring them to collect additional data. Under the current provisions of the PNR Directive, if collected by the air carrier, API will constitute an element of the PNR data which must be transferred to the Passenger Information Unit (PIU) – the unit set up by the Member State to collect and process PNR data – either together with PNR or separately, if the airline retains API by separate technical means.

API data are usually more reliable and include data fields (such as the date of birth) which allow for confirming the identity of the passengers. The PNR is a richer set of data, which reveals important information about passengers' travel behaviour as well as information leading to identification of previously unknown suspects, the establishment of links between members of criminal groups through the analysis of contact and payment details, the verification of the assumed 'modus operandi' of serious criminals and organised crime groups etc.

Main features of API and PNR Directives

	API Directive (Directive 2004/82)	PNR Directive (Directive 2016/681)
Purpose	Improving border control and combatting illegal migration	Prevention, detection, investigation and prosecution of terrorist offences and serious crime
Legal basis	Art. 62(2)(a) and 63(3)(b) Treaty establishing the European Community	Art. 82(1)(d) + 87(2)(a) Treaty on the Functioning of the European Union
Variable geometry	Member States and Schengen Associated Countries (CH, IS, NO – no airport in LI)	EU Member States (except for DK)
Geographic scope of data collection	Art. 2(b): external borders of the Member States with third countries	all extra-EU (mandatory) intra-EU (optional[130]) transit flights
Scope of data collection for law enforcement	Art. 6(1): in accordance with their national law MS may also use the data for law enforcement purposes	definition of terrorist offences as in the terrorism Directive and serious crimes referring to the categories of offences listed in Annex II of the PNR Directive
Type of data fields	Minimum requirements (i.e. MS can request carriers to collect more data): The number and type of travel document used, Nationality, Full names, The date of birth, The border crossing point of entry into the territory of the Member States, Code of transport, Departure and arrival time of the transportation, Total number of passengers carried on that transport, The initial point of embarkation.	Data as far as collected by air carriers (i.e. MS can only request carriers to transfer PNR data that they already have collected for their purposes) PNR record locator, Date of reservation/issue of ticket, Date(s) of intended travel, Name(s), Address and contact information (telephone number, e-mail address), All forms of payment information, including billing address Complete travel itinerary for specific PNR, Frequent flyer information, Travel agency/travel agent, Travel status of passenger, including confirmations, check-in status, no-show or go-show information, Split/divided PNR information, General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent), Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields, Seat number and other seat information, Code share information, All baggage information,

[130] All MS except AT and IE are applying this option

		Number and other names of travellers on the PNR, 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), All historical changes to the PNR.
Type of carriers	Art. 2(a): carriers that transport passengers by air	scheduled and non-scheduled flights
Authorities receiving data	authorities responsible for carrying out checks on persons at external borders	Passenger Information Units (PIUs)[131]
Applicable data protection framework	Regulation (EU) 2016/679 (General Data Protection Regulation)	Directive (EU) 2016/680 (Law Enforcement Directive)

[131] where air carriers collect API data, they transfer it to the PIUs (art. 8(2) PNR Directive)

Annex 7: Streamlining the transmission of API data to the carrier interface with an API router

To accommodate a general International Civil Aviation Organisation (ICAO) recommendation (SARP) for a **single-window API transmission**[132] and to reduce costs on the air-industry, this initiative builds on the **carrier interface and add an API router** to accommodate API data delivery by air carriers. This will enhance coherence with other EU instruments in the area of external border management involving the processing of passenger data, the carrier interface being a component of the imminent implementation of ETIAS and EES Regulations that is currently under development.

The imminent introduction of the Entry Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the future Visa Information System (VIS recast) will impose new obligations on air-carriers, martime-carriers and coach-carriers (trains are excluded) bringing passengers into the Schengen area.[133]

Before allowing third-country nationals in scope of these systems to board a plane, these carriers will have a new obligation to query the ETIAS, EES and VIS recast to determine if the passenger has the required valid travel authorisation (ETIAS) or whether the number of entries authorised by a visa has already been used. The 'verification query' uses certain traveller data.[134]

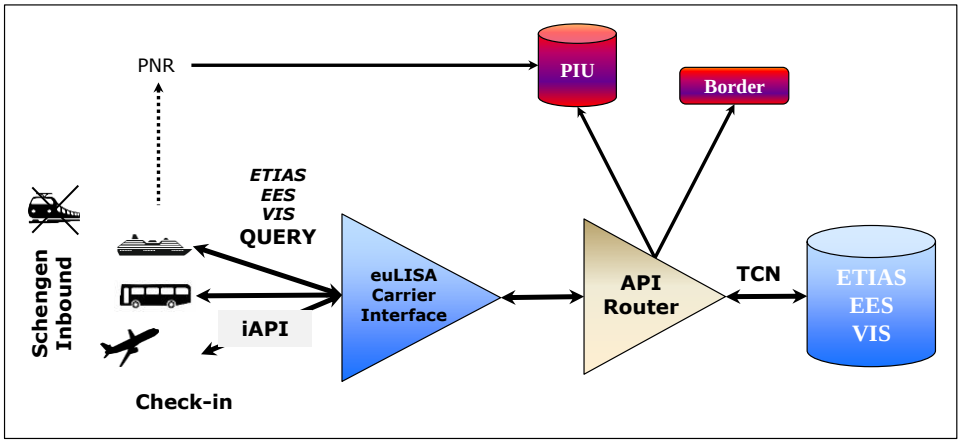
These carriers will transmit the ETIAS/EES/VIS recast query to a new centralised component at eu-LISA, called the **Carrier Interface**, that will centralise all connections of all concerned carriers.

---

[132] Annex 9 to the Chicago Convention, recommended practice 9.1: *Contracting States requiring the exchange of Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR) data from aircraft operators should create a **Passenger Data Single Window facility** for each data category that allows parties involved to lodge standardized information with a common data transmission entry point for each category to fulfil all related passenger and crew data requirements for that jurisdiction*.

[133] **Regulation 2017/2226 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; **Regulation 2018/1240 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; **Regulation (EU) 2021/1152 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008**, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 and (EU) 2019/817 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System .

[134] These data correspond to nearly all the Machine Readable Zone fields of the travel document (exception of the issuing State of the travel document) – see Article 13(3) of Regulation 2017/2226 and Article 45 of Regulation 2018/1240; see also Commission Implementing Regulation (EU) 2021/1217 of 26 July 2021 laying down the rules and conditions for verification queries by carriers, provisions for data protection and security for the carriers' authentication scheme as well as fall-back procedures in case of technical impossibility.



To minimise the burden on air carriers for systematic sending of API-data for inbound flights, for outbound flights and for selected intra-EU flights, API-data would only be sent to the carrier interface. The carrier interface would forward this API-data to the relevant border-control authorities and Passenger Information Unit(s) (PIU).

The transmission of API data to the carrier interface/API router would ensure that end-users, such as border guards, have access to fast and seamless access to API data they need to perform in the context of advanced border checks.

Establishing connections with carriers is a time-consuming task for national authorities. The current situation requires each Member State to have as many connections as there are commercial air carriers transporting passengers to their territory. Not all competent border authorities have the operational or technical capability to create the necessary connections. This solution for API-data delivery provides Member States with the possibility to 'sub-contract' the connections to eu-LISA and therefore save resources and increase efficiencies in the work of competent authorities.

National authorities would benefit from the support offered by the carrier interface/eu-LISA. For example, the carrier interface will support with basic quality assurance checks (e.g. structure and syntax of the message), which would leave national authorities with additional resources to focus on the content and analysis of API data. It would however not assess the content of the data, which will remain the responsibility and prerogative of national authorities receiving the data.

The **carrier interface will serve as a single connecting point between Member States and airlines**. It would drastically reduce the number of connections to establish and maintain from a Member States' perspective. Conversely, this would reduce the complexity for air carriers to maintain connections with all EU Member States and Schengen associated countries border management authorities and introduce economies of scale.

It establishes an EU approach for the transmission of API data to national authorities and enables them to increase the capacity required for API data processing and analysis (e.g. reallocate resources to improve operational planning, risk assessment, and operational responses).

While the carrier interface/router will support with basic quality assurance checks (e.g. structure and syntax of the message), it would however not assess the content of the data, nor touch on other aspects of the relationship between carriers and national authorities receiving the data (e.g. possible fining).

The task to establish connections with all carriers transporting passengers to the EU would be entrusted to **eu-LISA** as they have already started doing this for purposes of the EES/ETIAS/VIS2 query. eu-LISA will be responsible for the design, development and deployment and operations of the API router that should be established directly after the carrier-interface.

eu-LISA and the carrier interface will also be responsible for the **monitoring of flights carrying passengers**, reducing the probability that a flight did not comply with the obligation to send API data.

Following the concepts included in the Interoperability Regulations, the centralised delivery of API-data could in the future lead to using this data to query various databases (SIS, Europol data) via the European Search Portal.