Study supporting an impact assessment: potential effects of different possible measures on Advance Passenger Information

Final report

Written by Mathieu Capdevila, Veronika Vasileva,
Philip Gounev, Tatiana Kistruga, Angina Jugnauth,
Marie-Caroline Laurent, Guillaume-Xavier Bender,
Geoffrey Boomer, Giedre Kazlauskaite

September, 2021

EUROPEAN COMMISSION

Directorate-General for Migration and Home Affairs

Directorate D — Law enforcement and security

Unit D1 — Law enforcement cooperation

E-mail: home-api@ec.europa.eu

European Commission

B-1049 Brussels

Study supporting an impact assessment: potential effects of different possible measures on Advance Passenger Information

Final report

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Luxembourg: Publications Office of the European Union, 2021

PDF ISBN 978-92-76-41991-4 doi:10.2837/014167 DR-01-21-300-EN-N

September, 2021

Table of Contents

Abstract

Directive 2004/82/EC was adopted in 2004 and set out a common framework for the collection and transmission of Advance Passenger Information (API) at EU level. Based on shortcomings identified in the recent evaluation of the API Directive, the Study aims to support the impact assessment of the European Commission, specifically in the assessment of the potential effects of possible predefined measures. The Study assesses possible measures that would ensure processing of API data with clear rules and transparency and that are consistent with passengers' fundamental rights, interoperability of EU information systems for borders, security and migration management purposes, EU data protection requirements, and other existing EU instruments and international standards, while facilitating legitimate travellers. Five specific options are examined, including (i) possible measures on the scope of API data fields; (ii) possible measures on the scope of the application of API-related obligations on air carriers' flights; (iii) possible measures on extending the scope of API instruments to other transport modes (sea, rail, coach); (iv) possible measures on improving API data quality; and, (v) possible measures on integrating API into the framework for interoperability between EU information systems.

1 Introduction

This Draft Final Report represents the third final deliverable of the Study supporting an impact assessment regarding the potential effects of possible measures on advance passenger information (API), an assignment undertaken by **ICF** in cooperation with **Unisys** and **Lam-Lha**, on behalf of DG HOME.

This Draft Final Report is informed by:

- A review of desk research and available literature;
- Twenty-one interviews with 24 stakeholders at EU and international level;
- Six interviews at national level (border management authorities, law enforcement authorities and national travel data service institutions in four Member States);
- Results of the three surveys (industry, border management authorities, law enforcement authorities);
- Expert workshop on data protection to discuss the approach to the data protection impact assessment and analysis (3 November 2020). Results of the workshop fed into the assessment of the options in this Draft Final Report;
- Expert workshop with the European Commission, Study team and external experts (border management, PNR and data protection) to discuss fine-tuning the scenarios and initial assessments (13 January 2021).

1.1 Study objectives and scope

The 2020 evaluation[1] of Council Directive 2004/82/EC[2] on the obligation of carriers to communicate passenger data (API Directive) revealed several shortcomings stemming from the wording of the Directive and from the implementation of API systems by Member States. Since the adoption of the API Directive in 2004, the landscape changed significantly, with new instruments adopted for border management (e.g. European Travel Information and Authorisation System (ETIAS) and Entry-Exit System (EES) Regulations), law enforcement (e.g. Passenger Name Record (PNR) Directive), data protection (e.g. General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), and new international standards and practices on the use of API.

The general objective of the Study is to consider some specific aspects of a future instrument on API. It assesses possible measures that would ensure effective processing of API data for border management purposes, including facilitation of legitimate travellers and border control. The Study also assesses the processing of API data for law enforcement purposes, as currently the API Directive only mentions the possibility of using API data for law enforcement purposes, leaving to national legislation to regulate this use. Furthermore, the Study also examines the coherence of processing of API data with passengers' fundamental rights, interoperability of EU information systems for borders, security and migration management purposes, EU data protection requirements, and other existing EU instruments and international standards.

To reflect on possible measures that could strengthen uniform implementation and enhance the effectiveness of API processing, the study examines the following areas:

- Possible measures on the scope of API data fields;
- Possible measures on the scope of the application of API-related obligations on air carriers' flights;

[1] Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, available at: https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0082

- Possible measures on extending the scope of API instruments to other transport modes (sea, rail and coach);
- Possible measures on improving API data quality; and
- Possible measures on integrating API into the framework for interoperability between EU information systems.

The Study aims to provide evidence and analysis on selected possible measures and their potential impacts. For each option, the Study assesses its consistency with border management and law enforcement purposes, and whether it respects data protection and fundamental rights. The analysis and assessment of each of the scenarios is based on a cost-benefit analysis (CBA), as well as technical and operational feasibility, and a necessity and proportionality assessment of the measure, taking into account impacts on the right to privacy and protection of personal data, and risks to the rights and freedoms of data subjects.

The Study results will support the European Commission to elaborate and assess different policy options, which will feed into an impact assessment. The latter will be prepared before a legislative proposal is put forward, in order to assess the options that could be proposed and estimate their possible impacts.

The key elements of the scope of this Study are presented in Table 1.

Table 1. Key elements of the scope

Element	Within scope (maximum scope)	Outside scope
Geographical coverage	• Border management: 26 Schengen Member States: AT, BE, CZ, DE, DK, EE, EL, FI, FR, HU, IT, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, and 4 Schengen Associated Countries: CH, IS, LI, NO, as well as EU Member States that do not yet apply the Schengen acquis in full: BG, CY, IE, HR, RO • Law enforcement: all 27 EU Member States. The above are referred to as ‘Member States’ throughout this Report.	• Law enforcement : non-EU countries
Key legislative instruments	• API Directive, • PNR Directive, • European Travel Information and Authorisation System Regulation (ETIAS), • Entry-Exit System Regulation (EES), • Visa Information System Regulations (VIS), • Schengen Borders Code, • Schengen Information System Regulations (SIS), • Interoperability Regulations, • General Data Protection Regulation (GDPR), • Law Enforcement Directive (LED)	• Any other instrument not related to the EU acquis in the field of border management and or law enforcement.

Element	Within scope (maximum scope)	Outside scope
Transport modes and types of transportation	• Passenger transport services operators • Air carriers, including scheduled and charter flights • Maritime carriers • Train operators • International bus/coach service operators	• Freight/cargo outside scope
Planning horizon	January 2020 – December 2025	The evidence prior to 2020 is covered by the evaluation and the planning horizon is five years

1.2 Report structure

The remainder of this Draft Final Report is structured as follows:

- Section 2 provides an overview of the methodology;
- Section 3 describes the possible measures on API.

The following documents have been annexed to this Report:

- Annex 1: List of abbreviations;
- Annex 2: Glossary of terms;
- Annex 3: List of sources;
- Annex 4: Extension of the collection of PNR data for other modes of transport;
- Annex 5: Multi-Criteria Analysis (MCA);
- Annex 6: Approach to estimating costs;
- Annex 7: Analysis of the survey responses from carriers and national authorities (separate document);
- Annex 8: Evidence annex (separate document).

2 Methodology

The methodological approach for this research follows the Better Regulation Guidelines Toolbox on impact assessment[3]. It builds on the evidence collected and analysed for the 2020 evaluation and feedback on the inception impact assessment. Further information on the likely impacts of the policy options was gathered through additional stakeholder consultations, such as surveys and targeted in-depth interviews.

2.1 Data collection

Data collection consisted of interviews with stakeholders at EU level, industry representatives and national authorities. One survey targeted industry associations and carriers of the three modes of transport, while two others targeted national authorities (border management and law enforcement). The surveys ran from 20 October 2020 to 15 December 2020.

[3] https://ec.europa.eu/info/sites/info/files/better-regulation-guidelines-impact-assessment.pdf

2.1.1 Stakeholder interviews

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. These interviews build on the wide stakeholder consultations carried out with Member States during the Evaluation of the Directive in 2019-2020, as well as replies to the surveys (see 2.1.2.2). The selection of Member States was based on a mix of criteria such as geographic distribution and types of API systems implemented.

An overview of the stakeholders consulted is presented in Table 2 and Table 3.

Table 2. Overview of interviews at EU and international level

Type	Key stakeholders
EU institutions and agencies	• European Commission, DG MOVE (3 October 2020) • European Commission, DG JUST (6 November 2020) • European Commission, DG TAXUD (26 November 2020) • EBCGA (Frontex) (group interview) (20 October 2020) • Europol (9 November 2020) • eu-LISA (group interview) (15 October 2020) • FRA (group interview) (20 October 2020)
International and European industry associations	• International Air Transport Association (IATA) (group interview with A4E) (16 November 2020) • Airlines for Europe (A4E) (16 November 2020) • European Regions Airline Association (ERAA) (9 November 2020) • European Business Aviation Association (EBAA) (3 December 2020) • International Road Transport Union (IRU) (21 January 2021) • Community of European Railway and Infrastructure Companies (CER) (30 October 2020) • ECSA, Interferry, Cruise Lines International Association (CLIA) (group interview) (11 November 2020, 10 December 2020)
Carriers/industry stakeholders	• Svensk Sjöfart (SE) (25 November 2020) • Amadeus (5 November 2020) • SITA (5 November 2020) • Travelport (5 November 2020)
International organisations	• International Civil Aviation Organisation (ICAO) (21 October 2020) • World Customs Organization (WCO) (17 December 2020) • International Maritime Organization (IMO) (15 January 2021)
NGOs	• Access Now (9 November 2020)

Table 3. Overview of interviews at national level

Member State	Authority
Finland	• National Bureau of Investigation, Passenger Information Unit (PIU) • Finnish Border Authority
Germany	• Border management authority (air borders)
France	• *Service national des données de voyage*, *Secrétariat Général aux Affaires Etrangères*, Permanent Representation to the EU

Member State	Authority
Romania	• PIU • Romanian Border Police

A summary of stakeholder views can be found in **Annex 8**.

2.1.2 Surveys

2.1.2.1 Industry survey

The industry survey was successfully uploaded onto the Voxco© platform and was piloted internally during October 2020.

The industry survey was launched on 20 October 2020. It targeted three different industry associations and carriers (air, maritime, land and rail) and was initially disseminated with the help of the respective industry associations. IATA and AIRE were actively involved in its dissemination among their members. Similarly, industry organisations for other modes of transport were invited to participate in the survey and to distribute the survey among their members. A total number of 27 stakeholders provided complete responses[4], of which 20 were air carriers, four land carriers and three maritime industry representatives. The air carriers included some of the largest carriers in Europe (e.g. KLM, Air France) and globally (United), and both national and low-cost carriers, primarily operating inbound extra-EU flights and not EU based.

The survey closed on 15 December 2020. An analysis of the responses to the industry survey can be found in **Annex 7**. For the purposes of this Study, the responses from air, maritime and land industry associations and carriers were analysed separately.

2.1.2.2 Surveys of national authorities

Two surveys targeting border management authorities and law enforcement authorities of all Member States (and Schengen Associated Countries where relevant) were disseminated with the support of the European Commission and the Council Working Groups (Frontiers and IXIM). The survey was launched on the 23 October 2020 and closed on 15 December 2020. Member States that responded (either online or by completing a pdf document) were:

- Twenty border management authorities (Austria, Bulgaria, Czech Republic, Cyprus, Estonia, France, Finland, Germany, Hungary, Italy, Latvia, Luxembourg, Lithuania, Poland, Romania, Slovenia, Slovak Republic, Spain, Iceland and Switzerland);
- Fifteen law enforcement authorities (Belgium, Czech Republic, Cyprus, Denmark, France, Hungary, Italy, Ireland, Latvia, Malta, the Netherlands, Romania (2 authorities), Slovak Republic and Sweden).

An analysis of the responses to the national surveys can be found in **Annex 7**.

2.2 Approach to estimating costs

The approach to estimating costs is presented in Annex 6 attached to this Report.

2.3 Multi-Criteria Analysis

As per Toolbox #63 of the Better Regulation Guidelines, the MCA method can help to establish preferences between a sub-set of scenarios by reference to an explicit set of objectives and measurable criteria. MCA allows aggregation of a complex set of evidence

[4] The industry survey carried out for the 2020 evaluation gathered 33 complete responses.

(monetary, quantitative, qualitative) against individual criteria to provide an assessment of the overall performance of different options/scenarios.

The first step of the MCA was to define the criteria for the assessment and to set the respective scoring or weighting. The main criteria set for assessing the options and possible measures for a revision of the API Directive were:

- Effectiveness;
- Efficiency;
- Coherence;
- Respect for the fundamental rights of data subjects including data protection.

An outline of the key elements of the assessment, as well as a pre-assigned individual and overall weight, can be found in Annex 5. The MCA follows a structured approach whereby weighting is pre-assigned to each criterion. Given the importance of each of the four criteria, equal weights of 25% were assigned to each criterion. Each criterion is then composed of a number of components and each component is assigned individual weight. More details as to how each component was assessed can be found in **Annex 5**.

3 Possible measures on API

This section presents five policy options in relation to possible measures on API in the main areas identified in the Terms of Reference:

- Scope of API data fields (policy option 1);
- Scope of the obligation to communicate API data for air transport (policy option 2)
- Scope of the obligation to communicate API data for other transport modes (policy option 3);
- Data quality (policy option 4);
- Integrating API into the framework for interoperability between EU information systems (policy option 5).

3.1 Baseline

This section presents the current state of play of the implementation of the current API Directive (Baseline 0) as well what will happen following the implementation of ETIAS and EES (VIS) Regulations in or after 2022 (Baseline '+').

3.1.1 Purpose of API data collection and processing

Article 1 of the API Directive states that the purpose of API data collection and processing is to improve border controls and to combat irregular immigration by the transmission of advance passenger data by carriers to the competent national authorities.

The API Directive does not specify the types of flights for which data should be collected, instead leaving it to Member States to determine the inbound extra-Schengen flights for which carriers should transfer data. API data are thus collected for border control purposes on extra EU/Schengen inbound flights[5].

The API Directive allows the collection and transfer of API data for law enforcement without specifying flights or routes and without a clearer definition of 'law enforcement'[6].

[5] Theoretically, API data could be collected on an ad hoc basis for intra-Schengen flights in circumstances where Member States temporarily reintroduce border controls at internal borders (Chapter 2 of Title III of the Schengen Borders Code).

[6] Recital 12 API Directive provides that "*whereas it would be legitimate to process the passenger data transmitted for the performance of border checks also for the purposes of allowing their use as evidence in*

In practice, the 2020 evaluation showed that Member States took this to include purposes such as internal security and public order, to fight terrorism, to protect national interests and other national security concerns. This is a different approach from that adopted in the PNR Directive, whereby the collection and use of data is limited to the 'prevention, detection, investigation and prosecution of terrorist offences and serious crime' (Annex 2 PNR Directive). Based on national legislation and other EU instruments (e.g. PNR Directive), Member States may already receive API data for law enforcement purposes on extra-EU outbound, intra-EU and domestic flights, insofar as they are collected by carriers for their own business purposes (Article 8 PNR Directive).

3.1.2 API data elements

WCO/IATA/ICAO Implementation Guidelines on API[7] provide a list of data that can be requested by national authorities in respect of inbound or outbound flights. The guidelines refer to a maximum set of data that could be included in the passenger list (PAXLST) message to be used for the transmission of such data by the carriers (see section 3.1.3). The PAXLST message comprises data relating to the flight and to each individual passenger and crew member. It is divided into three categories:

- Core data elements as found in the 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.

Accordingly, '*The passenger data corresponds to those items of data that currently appear on machine-readable passports, other official travel documents or those which may be available in the transporting carrier's reservation system'*. 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*'[8].

Appendix IIA on the PAXLST message implementation guide makes no distinction between passengers and crew members[9].

3.1.2.1 Passenger information

The API Directive does not impose an obligation on Member States to request the collection and transmission of API data but, rather, provides the option for Member States to request those data from air carriers. The list of API data fields provided in Article 3(2) of the API Directive includes both passenger data (number and type of travel document, nationality, full name, date of birth) and flight data (border crossing point of entry, code of transport, departure and arrival time, total number of passengers carried, initial point of embarkation). This list is neither exhaustive nor mandatory, giving each Member State the right to request additional data elements in line with national legislation. The API Directive does not refer to crew members.

The list of data elements listed in the API Directive is not aligned with the list of recommended data as per international standards, including the core data as per the MRZ fields (see Table 4 in section 3.1.10).

proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (ordre public) and national security, any further processing in a way incompatible with those purposes would run counter to the principle set out in Article 6(1)(b) of Directive 95/46/EC".

[7] 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.

[8] WCO/IATA/ICAO Implementation Guidelines, para 8.1.3.

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

However, Member States request additional data fields other than those listed in the API Directive[10]. These include data such as gender, nationality, issuing State and expiry date of the travel document, seat and baggage information, and (in some cases) visa information.

3.1.2.2 Crew information

Data on crew are not captured by either the API Directive or the PNR Directive. As part of the ICAO PAXLST message standard, States have the option to request crew data, which is echoed in Annex 9 to the Chicago Convention, '*API involves the capture of a passenger's or crew member's biographic data and flight details'*.

Likewise, international standards on maritime transport prescribe the collection of crew data[11].

According to the Schengen Borders Code (Annex VII), holders of a pilot's licence or a crew member certificate are subject to specific conditions related to border checks.

3.1.3 API data format

API messages contain a limited set of biographical data about each traveller, normally confined to the data contained in the MRZ of their travel document, as well as flight information. Passenger and crew API data are generally transmitted to Member States using the UN/EDIFACT PAXLST message format following the WCO/IATA/ICAO Implementation Guidelines. The Guidelines define how the PAXLST message segments are to be used to send the API data[12] and, together with the UN/EDIFACT PAXLST standard, are regularly updated (latest in 2016). The most recent versions of the PAXLST standard are usually compatible with previous versions.

An updated PAXLST message format does not equate to uniform implementation and use by all carriers. The implementation of the PAXLST versions, both by carriers and receiving competent authorities, can vary, sometimes within the same country. Depending on the version of the PAXLST standard in use, collection of certain API data fields would imply additional technical and operational adjustments (e.g. passenger luggage weight is part of one of the latest PAXLST revisions). In other instances, a service provider reported instances whereby one authority requests an API message in one PAXLST format, while another authority within that same Member State requires it in a different format.

3.1.4 API data capture

The API data collection method depends on carriers' technical capacities, the type of check-in (online check-in versus airport check-in), or the airport of embarkation. API data are captured during the check-in process (i.e. within 48 hours prior to departure) but can be collected several weeks in advance if requested at booking or via self-check-in.

Currently, a passenger has several check-in options:

- **Manual data** entry by the carrier at check-in counters (e.g. for travel documents without MRZ or when additional data not contained in the MRZ are required);
- **Self-declaration** – entered manually either through the carrier's website/online/app check-in process;
- **Self-declaration** via a mobile app or a kiosk using the optical character recognition (OCR) of the MRZ information from a picture of the travel document (the passenger submits the OCR unsupervised);

[10] As evidenced by the 2020 evaluation and data collected for this Study.

[11] IMO, Convention on Facilitation of International Maritime Traffic (FAL Convention), Crew List (FAL Form 6).

[12] https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/appendix-iia-paxlst-message-implementation-guide-2016.pdf

- **Automated capture** of the information from the MRZ of the travel document via an OCR at the check-in desk (the data are collected and verified as corresponding to the person presenting the document).

As yet, carriers do not capture of the biographical information from the MRZ of the travel document via the reading of the RFID chip data (via an app, a kiosk or a reader used by the check-in agent). Some carriers[13] are in the process of introducing such capabilities. Several carriers already offer the possibility for passengers to use a biometric token to facilitate baggage drop, entry into airside, boarding/etc. (with three others planning to offer this solution)[14]. Even if several options can be supported by carriers, these options are not necessarily available throughout the carriers' systems, as the check-in process depends on the local capabilities of the departure airport and on the type of route.

3.1.5 Transmission of API data

Data gathered at check-in are usually stored in carriers' Departure Control Systems (DCS) and transmitted automatically to national authorities at departure or flight reconciliation time. Carriers normally transmit the API data at the actual time of departure (ATD). In case of transmission failure, national authorities can request re-transmission of the data up to 48 hours after the ATD. The time of API transmission varies greatly, ranging from 48 to 24 hours before the planned time of the departure, after check-in, or at flight closure[15].

Passenger and crew (where requested) API data are generally transmitted as two separate messages to the Member States. Where API data are collected for the flight, they also need to be transmitted to the PIUs established under the PNR Directive.

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).

Several Member States offer a web portal where carriers can manually enter the API data of passengers and crew by uploading pre-formatted files. This portal solution is used by small airlines, private flights, and charter flights. As an alternative to providing a web portal, several Member States support sending API files via email.

Depending on the state of implementation of API systems and PIUs in Member States, API data transmission from carriers to Member States falls into one of the following three scenarios:

- Transmission to PIUs, which act as a Single Window (receive API and PNR data and forward the data to the relevant authorities);
- Transmission to PIUs and border control authorities - carrier sends the API data twice;
- Transmission only to the border control authorities, as not all Member States have implemented the PNR Directive and set up a PIU[16].

3.1.6 Ensuring API data quality

Only some Member States' authorities perform data quality checks prior to processing the data to determine whether human intervention is required[17]. Existing methods for

[13] Some industry survey respondents.

[14] As per Five respondents to the industry survey.

[15] 2020 evaluation results.

[16] European Commission, Staff Working Document on the review of Directive 2016/681.

[17] 2020 evaluation: BG, CH; CZ, DK; ES; FR; PL; PT; SI; SK; UK; in EE, PL, IT, IS and NO perform manual checks; in HU, quality checks are occasional; neither IE nor NL have specific data quality verification mechanisms in place.

running systematic data quality processes range from a certification process for carriers[18] to checks on data formats[19], data completeness[20] and accuracy[21].

The increase in the use of manual self-declaratory methods (e.g. online booking or manual data entry at check-in by the passenger) to capture API data can result in poor data quality[22].

Many carriers' platforms (either online or in-person check in) do not conduct automatic semantic or syntax checks of the self-declared data entered, which allows for incorrect or incomplete data to be entered[23].

The timing of API data transfer has an impact on completeness - and therefore quality - of the data transferred. Member States also receive the data at multiple points in time, with some receiving them more than once[24].

While the API Directive provides that Member States shall impose sanctions on carriers that have not transmitted data or transmitted incomplete or false data, most Member States have not imposed any such sanction[25]. In 14 Member States, fines have been imposed for the violation of obligations related to the transmission of API data[26]. Different amounts are applicable for carriers failing to collect and correctly transmit API data (ranging from EUR 100 in Germany to EUR 500,000 in Ireland).

3.1.7 API data collection on type of flights

In terms of types of flights, the API Directive does not specify for which flights data should be collected but leaves this to Member States to determine for which inbound extra-Schengen flights carriers should transfer data. Therefore, currently, API data is collected for border control purposes on extra EU/Schengen in-bound flights.[27]

Under the API Directive, carriers have the obligation to transmit (passenger) API data on selected extra-EU/Schengen inbound flights. Most Member States collect (or are planning to collect) API data on all extra-EU inbound flights[28], with several collecting data on selected flights[29] based on a risk analysis of routes from an irregular migration or terrorism perspective. Some States do not yet have a fully implemented API system (e.g. Cyprus, Greece and Norway).

Several Member States have extended the scope of API collection to outbound extra-EU/Schengen flights[30], a requirement not expressly covered by the API Directive. In comparison, Annex VI of the Schengen Border Code, in its section 2.1 on procedures for checks at international airports, indicates that passengers who board on a flight to a third country are subject to an exit check. Likewise, Article 2(1) of the PNR Directive mentions the collection of PNR data to extra-EU flights, covering both arriving and departing flights to/from outside the EU.[31].

[18] 2020 evaluation: BG, FR, LU.

[19] 2020 evaluation: BG, PL, SI, CH.

[20] 2020 evaluation: SK, CH.

[21] 2020 evaluation: BG, LT, LV.

[22] Evaluation of Council Directive 2004/82, p. 130.

[23] CRM Feasibility Study Report; Interviews with industry;

[24] 2020 evaluation: DK, EE, ES, IE, LT, PL, PT, SK.

[25] 2020 evaluation: BE, BG, CY, DK, EE, EL, FR, IE, LU, NL, PT, SE, SI, SK, IS, NO, UK.

[26] 2020 evaluation: AT, CZ, DE, ES, FI, HU, HR, IT, LV, LT, MT, PL, RO, CH.

[27] Theoretically, API data could be collected on an ad hoc basis for intra-Schengen flights in circumstances where Member States temporarily reintroduce border controls at internal borders (as per Chapter 2 of Title III of the Schengen Borders Code).

[28] 2020 evaluation: AT, BG, CZ, EE, ES, FI, HR, HU, IE, IT, LT, LV, MT, NL, PT, RO, SE, SI, IS

[29] 2020 evaluation: DE, DK, FR, LU, NO, PL, CH.

[30] 2020 evaluation: BE, BG, DK, EE, FI, FR, LT, PL, RO, SI, SK.

[31] Yet Article 2(1) of the PNR Directive mentions the collection of PNR data to extra-EU flights, covering both inbound and outbound arriving and departing flights to/from outside the EU.

As part of the implementation of the PNR Directive, several Member States also collect API data (as part of the PNR message) for intra-EU flights, when this information is already available in the carriers' systems[32].

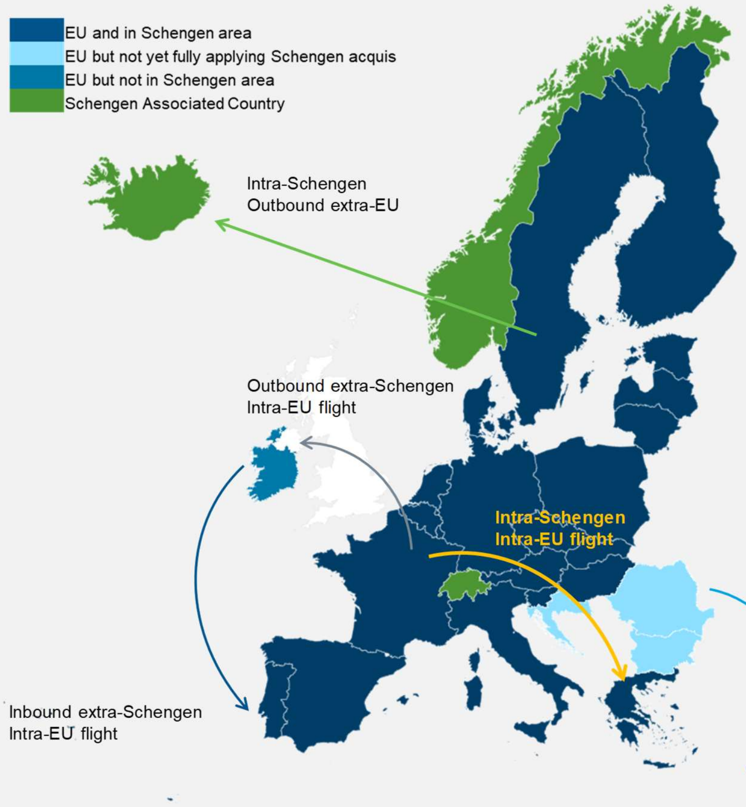
Several Member States appear to collect API data for domestic flights – an option foreseen in neither the API Directive nor in the PNR Directive.

Figure 1. ***Extra-EU versus extra-Schengen flights***

Extra-EU and extra-Schengen inbound flights can refer to different geographical realities with different passenger data requirements. As illustrated below, a flight from Ireland to Portugal is an extra-Schengen inbound and thus subject to the same Schengen border controls as a flight from the US even though it is an intra-EU flight.

Intra-EU flights may also be extra-Schengen outbound (e.g. France to Ireland), intra-Schengen (France to Greece) or 'non-Schengen' (e.g. Bulgaria to Cyprus).

Similarly, an extra-EU outbound flight may still be intra-Schengen (e.g. a flight from Sweden to Norway).



Source: ICF and Unisys.

The API Directive defines external borders as 'the external borders of the Member States with third countries'[33]. This provision has led to different interpretations of the Directive's geographical scope of application[34]:

- The Directive's obligations apply to flights coming from outside the EU.

[32] BG, DK, FR, LT, SI, SK, IS*.

[33] Article 2(b) Directive 2004/82.

[34] European Commission, Staff working document, Evaluation of the Council Directive 2004/82.

- Following this interpretation, carriers operating flights which depart from a Schengen Associate Country are required to transmit information on passengers when they are flying into an EU Member State.
- The Directive's obligations apply to flights coming from outside the Schengen area, irrespective of whether or not the country of origin belongs to the EU.
- The Directive's obligations apply to flights coming from outside the Schengen area only if the country of origin does not belong to the EU.

3.1.8 API data collection from types of carriers

The API Directive does not explicitly define the modes of transport for which API data should be collected. However, Article 2(a) defines 'carrier' as any natural or legal person whose occupation it is to provide passenger transport by air only.

Member States do not systematically collect API data from all air carriers. Most States request API data from all air carriers[35], while a share of States request it from certain air carriers[36]. Data are not typically collected for charter, business and cargo flights.

Currently, the API Directive only sets minimum standards for Member States to request API data, with Member States free to request similar data from other transport carriers, such as maritime or rail transport carriers. API data are collected from maritime carriers in 10 Member States[37], from rail operators in four Member States[38], and from coach carriers in one Member State[39].

3.1.9 API data processing and connection with other systems

When a competent authority receives API data, either from the PIU or through a dedicated transmission from the carrier, a screening process takes place against databases such as watchlists, SIS, SLTD and Travel Documents Associated with Notices (TDAWN) databases, as well as information managed by the Europol Information System (EIS) and the European Criminal Records Information System (ECRIS). As in the case of PNR, API data can be checked against risk profiles/targeting rules.

Currently, practices in the Member States differ substantially in their use of API data to query systems and databases[40]:

- Most Member States[41] now check API data against their SIS national copy[42], with four querying the SIS central system directly (DK, FI, NO, SI);
- Eighteen Member States check API data against the SLTD database (or similar national databases)[43].

Member States noted the national (e.g. watchlists and risk profiles, criminal investigation registers), EU (e.g. EIS, VIS, SIS) and international (e.g. SLTD) databases against which API data are checked. All consulted Member States confirmed using national databases, with SIS and the SLTD database the next most commonly used.

[35] 2020 evaluation: AT, BG, CY*, CZ, DK, EL*, ES, FI, FR, HU, IE, LT, LU, LV, MT, SE, SI, IS, UK (*planned API system, not yet fully operational).

[36] 2020 evaluation: BE, DE, EE, IT, HR, NL, PL, PT, RO, SK, CH, NO* (*planned API system, not yet fully operational).

[37] 2020 evaluation: AT, BE*, EE, ES, FI, FR, HU, IS*, MT, NO*. (*Planned API system).

[38] 2020 evaluation: EE, FI, FR, UK.

[39] 2020 evaluation: AT.

[40] 2020 Evaluation of Council Directive 2004/82.

[41] 2020 evaluation: AT, BE, CZ, DE, DK, EE, FI, FR, HR, HU, LT, LU, LV, MT, NL, PL, RO, SE, SI, SK, CH, NO*, IS*, UK (*Planned API system).

[42] Meaning that, in substance, there is a uniform application regarding the checks of SIS with API data (as national copy of SIS or the Central database of SIS contain same data).

[43] 2020 evaluation: BE, DE, DK, EE, FI, FR, HR, IE, LT, LU, NL, SE, SI, SK, UK, CH, RO, NO* (*Planned API system).

One country mentioned being in the process of connecting to additional databases, such as VIS (SI).

Verification against these databases is based on various data fields, most commonly name, first name, date of birth, and number of travel document.

3.1.10 Passenger Name Record (PNR) Directive

PNR data is unverified information provided by passengers, collected by air carriers in the normal course of their business, with the purpose of enabling reservation and delivering transport services. The content of PNR data varies depending on the service requested by the passenger (e.g. type of meals, baggage request) and may contain information on dates of travel, itinerary, ticket information, contact details, travel agent, means of payment, seat number and baggage information. The PNR Directive also mandates the transfer of API data as part of PNR data by the 'push method', where those data are collected by air carriers in the normal course of their business (Annex I PNR Directive).

The review of the application of the API Directive found that the large majority of Member States have established operational PIUs, with 24 of 26 Member States having notified full transposition[44]. Spain has also since notified full transposition (in September 2020). All Member States have established Information Units ('PIUs'), the majority of which are fully operational. Four Member States did not fully transpose the Directive[45,46].

While the primary objective of the PNR Directive is to act as a law enforcement tool, the API Directive allows the use of API data for law enforcement purposes, in addition to its main objectives of border control and prevention of irregular migration. While Annex II to the PNR Directive details the list of serious offences and crimes for which PNR data can be used, the API Directive has not clarified the law enforcement purposes for which API data can be used. In the context of the PNR Directive, the use of API data enhances PNR data by verifying the identity of an individual. However, in terms of geographical scope, the PNR Directive only applies to EU Member States (except DK[47]), while the API Directive builds on the Schengen acquis[48]. Additionally, the Directives do not apply to the same types of flights. According to the PNR Directive, Member States have the possibility to extend the obligation to transmit PNR data to air carriers operating intra-EU flights – for the purposes of prevention, detection, investigation and prosecution of terrorist offences and serious crimes. The API Directive does not mandate the collection of API data on such flights.

[44] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=NIM:288563. European Commission, 2020, Staff Working Document, PNR Directive Review Report, p.5 and 9, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf.

[45] European Commission, 2020, Staff Working Document, PNR Directive Review Report, p.5 and 9, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf.

[46] *European Commission, 2020, Staff Working Document, PNR Directive Review Report, p.5 and 9, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf.ibid.*

[47] Denmark has adopted national legislation with the same effect as the PNR Directive.

[48] European Commission, 2020, Staff Working Document, Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), p. 46.

Table 4. Comparison of main passenger data elements requirements in the API Directive, international standards, PNR Directive and other EU systems

Data elements	API Directive	MRZ[49]	WCO/ICAO/ IATA API Guidelines	PNR Directive	SIS (police)	EIS	SLTD	TDAWN
Biographical data								
Full name	■			*	■	■		■
Surname/given name(s)		■	■	*	■	■		■
Date of birth	■	■	■		■	■		
Place of birth			■		■	■		
Nationality	■	■	■	*		■		
Additional nationalities					*	■		
Gender		■	■		■	■		
Travel document data								
Travel document number	■	■	■	*	■	■	■	■
Travel document type	■	■	■		■		■	
Issuing State or organisation of the official travel document		■	■	*	■	■	■	■
Expiry date of official travel document		■	■	*		■	■	
Other document number used for travel			■					
Type of other document used for travel			■					
Visa number			■					
Issue date of the visa			■					
Place of issuance of the visa			■					
Additional passenger information								
Seating information			■	■ *				
Baggage information			■	■ *				
Traveller status			■	■ *				
PNR locator number			■	■ *				
Address of primary or permanent residence			■		■	■		
Destination address			■					
Biometric data								
Facial image					■			
Fingerprints					■			

■	Data element included
*	In SIS, information on nationality can be included (not mandatory)

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

3.1.11 Collection and transfer of passenger and crew data in the maritime transport sector

The baseline analysis considers the existing framework for passenger and crew data collection in the maritime transport sector:

- Article 26 of the Convention Implementing the Schengen Agreement (CISA) provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry.
- As per Annex VI Chapter 3 on maritime carriers of the Schengen Borders Code (Regulation 2016/399/EU), crew and passenger information must be transmitted by carriers to border authorities as a list 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. These data must be transmitted at least 24 hours prior to the scheduled arrival of the vessel. Passenger and crew data contained in the FAL forms do not fully correspond to the passenger data listed in the API Directive (see Table 5).
- There are obligations to collect passenger information (passenger manifests) as per Directive 98/41/EC (PAX Directive) on the registration of persons sailing onboard passenger ships operating to or from ports of the Member States, as amended by Directive 2017/2109 (entered into force on 21 December 2019). The latter provides that a passenger ship should record the family name of each person on board, their forename(s), gender, nationality, date of birth and, if provided by the passenger, a contact number in case of an emergency, as well as information concerning special care or assistance that might be needed in an emergency (Article 5 PAX Directive).
- Directive 2010/65/EU[50] (Reporting Formalities Directive (RFD) provides that the reporting formalities (e.g. FAL 5, FAL 6, crew and passenger manifest) should be transmitted electronically via the National Maritime Single Window (NMSW). Article 4 provides for the prior notification of at least 24 hours of arrival into ports situated in a Member State, including the passenger list. It sets an obligation for Member States to establish NMSWs for reporting formalities from ships arriving and/or departing from ports. The passenger and crew information required by the FAL forms does not fully correspond to the passenger data listed in the API Directive (see Table 5).
- Following the Council's 'Valetta Declaration' of 2017, calling for the digitalisation and administrative simplification of the maritime sector, the co-legislators adopted Regulation (EU) 2019/1239, establishing an EMSW environment[51]. It was intended to harmonise the interfaces available to ships' operators to provide information and to create a standardised maximum dataset. It will replace Directive 2010/65/EU from 15 August 2025. The Regulation will provide a harmonised framework and tools for the transmission of passenger data for maritime transport.

[50] Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:283:0001:0010:EN:PDF

[51] https://ec.europa.eu/transport/modes/maritime/digital-services/e-maritime_en

Table 5. Comparison of main passenger data elements in the API Directive, international aviation and maritime standards

Data elements	API Directive	MRZ[52]	WCO/ICAO/ IATA API guidelines	FAL form 5 (crew)	FAL form 6 (passenger)
Biographical data					
Full name	▨				
Surname/given name(s)		▨	▨	🟦	🟦
Date of birth	▨	▨	▨	🟦	🟦
Place of birth			▨		🟦
Nationality	▨	▨	▨	🟦	🟦
Additional nationalities					
Gender		▨	▨	🟦	🟦
Travel document data					
Travel document number	▨	▨	▨	🟦	🟦
Travel document type	▨	▨	▨	🟦	🟦
Issuing state or organisation of the official travel document		▨	▨	🟦	🟦
Expiry date of official travel document		▨	▨	🟦	🟦
Other document number used for travel			▨	🟦	
Type of other document used for travel			▨		
Visa number			▨		🟦
Issue date of the visa			▨		
Place of issuance of the visa			▨		
Additional passenger information					
Seating information			▨		
Baggage information			▨		
Traveller status			▨		🟦
PNR locator number			▨		
Address of primary or permanent residence			▨		
Destination address			▨		

▨ Data element included

🟦 Data element included

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

3.2 Baseline+ (status quo from 2022)

Revisions to an instrument regulating the collection and transfer of API data at EU level need to account for the implementation of other border control systems that are due to become operational in the near future. The **EES (VIS[53]) and ETIAS** Regulations are due to be implemented by 2022. In that context, a sub-set of API data (data from the MRZ, route and transport details, Member State of entry) will be used, where applicable, to check whether a third-country national boarding an aeroplane, sea vessel or coach, and holding a short-stay visa issued for one or two entries, has already used the number of entries authorised by their visa (EES) and whether a third-country national subject to the travel authorisation requirement is in possession of such authorisation to enter the Schengen area (ETIAS).

3.2.1 Entry Exit System (EES) (including amended VIS) and European Travel Information and Authorisation System (ETIAS)

3.2.1.1 EES (and VIS)

The **EES**[54] is an information system interlinked with the VIS, enabling Member States to identify third-country nationals who stay in the Schengen area, Bulgaria or Romania beyond the authorised time. The EES will require entry and exit border checks on all non-EU citizens admitted for a short stay (maximum of 90 days within any 180-day period), with or without a visa (visa holders or visa exempt). Third-country nationals in possession of a long-stay visa or a valid residence permit ('residence permit holders') do not fall within the scope of the EES[55].

Prior to the EES, international carriers must manually check if a third-country national travelling to the Schengen area has a valid visa, as per the obligation under CISA[56]. With the implementation of the EES, the recording of entries and exits in the Schengen area will replace the manual stamping of passports and enable carriers to automatically detect overstayers. The EES Regulation foresees a web service to allow carriers to verify, before boarding, whether a traveller holding a Schengen short-stay visa issued for one or two entries has already used the number of entries authorised by their visa[57]. Carriers will provide the following personal data of third-country nationals subject to a visa requirement (corresponding to the MRZ of the travel document)[58] to the web service in order to enable it to perform this verification:

a) surname (family name), first name(s) (given names), date of birth, nationality or nationalities, sex;

b) type and number of the travel document(s) and the three-letter code of the issuing country of the travel document(s);

c) date of expiry of the validity of the travel document(s).

The web service will then provide carriers with an OK/NOT OK answer. However, this shall not constitute a decision to authorise or refuse entry into the Schengen area -

[53] The recent proposal amending VIS Regulation (COM(2018) 302 final) introduced the requirement for carriers to query the VIS with regard to short-stay visas, long-stay visas and/or residence permits. It proposes an amendment to the EES Regulation by obliging carriers to use the web service to verify whether a short-stay visa is valid, including if the number of authorised entries have already been used or if the holder has reached the maximum duration of the authorised stay or, as the case may be, if the visa is valid for the territory of the port of destination of that travel.

[54] 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.

[55] These categories are covered by the VIS Regulation (2021/1134).

[56] Article 26(1) of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000.

[57] Article 13(3) of the EES Regulation.

[58] Article 16(1), points (a), (b) and (c) of the EES Regulation.

Article 14(2) of the Schengen Borders Code states that entry may only be refused by a substantiated decision stating the precise reasons for the refusal. The decision should be made by an authority empowered by national law (i.e. the border guard) and not by automated means.

The draft Implementing Regulation for carriers refers to web services as 'carrier interface'[59] (i.e. the logical grouping of the ETIAS and EES carrier system interface services into a logically combined service, as seen by the carriers).

Even though the types of carriers are not explicitly mentioned in the EES Regulation, the reference to the CISA whereby rail carriers are excluded from the requirement to verify whether a third-country national travelling to the Schengen area has valid travel documents, the Regulation is considered to have inherited the same approach. This is supported by the clear mention in the ETIAS Regulation of air carriers, maritime carriers and international carriers transporting groups overland by coach.

3.2.1.2 ETIAS

The **ETIAS**[60] will enable the advance assessment of risks that may be posed by visa-exempt travellers entering into Schengen[61] and, if necessary, deny them authorisation to travel. Visa-exempt travellers will have to make an online application (via a dedicated website or app) for ETIAS travel authorisation prior to travelling to the Schengen area[62]. Prior to boarding, air carriers, maritime carriers and carriers transporting groups overland by coach shall send a query to the ETIAS Information System to verify whether or not third-country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation. For carriers transporting groups overland by coach, such verification will be optional for the first three years following the ETIAS entry into operation, and the provisions on penalties shall not apply[63].

Secure access to the carrier gateway referred to in Article 6(2) point (k) of the ETIAS Regulation, including the possibility to use mobile technical solutions, will allow carriers to proceed with the query prior to boarding. The carrier will provide the data contained in the MRZ and indicate the Member State of entry. The query will thus contain (almost) the same data fields as those received under the API Directive (see Table 6). The data on crew are exempt from ETIAS requirements[64]. No obligation to query ETIAS via the carrier gateway is imposed on carriers in the case of airport transit.

Similar to the EES, upon querying the central ETIAS system via a carrier gateway, carriers will receive an OK/NOT OK response. The carrier gateway shall make use of a separate read-only database updated daily via a one-way extraction of the minimum necessary sub-set of data stored in the ETIAS. eu-LISA[65] will be responsible for the security of the carrier gateway and the personal data it contains, as well as the process of extracting the personal data into the separate read-only database[66].

Where carriers complied with the obligation to query the carrier gateway prior to boarding and acted on the answer received from the system, the carrier will not be

[59] Interview with EU Agency representatives on 20 October 2020.

[60] 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.

[61] ETIAS enables consideration of whether the presence of third-country nationals exempt from the visa requirement when crossing the external borders would pose a security, illegal immigration, or high epidemic risk (Article 1 ETIAS Regulation).

[62] The application will collect a set of personal data as well as answers to a list of questions (Article 17 ETIAS Regulation).

[63] Article 45(9) of the ETIAS Regulation.

[64] Article 2(2) (i) of the ETIAS Regulation, referring to points a) to f), Article 4, Regulation 539/2001 (exemptions for air and sea crew).

[65] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

[66] Article 45(4) of the ETIAS Regulation.

subject to further penalties if a passenger is refused at the border. This will be possible through the requirement that eu-LISA keep logs of all processing operations as proof that the carrier undertook the check. These logs will show the date and time of each operation, the data used for interrogation, the data transmitted by the CG and the name of the carrier. The logs shall be stored and access protected according to data protection rules[67].

An implementing act is currently being developed by the European Commission in close collaboration with eu-LISA to clarify the conditions for carriers' access and use of the CG.

The ETIAS is thus an electronic travel system (ETS) whose aim is to expedite pre-vetting and acceptance of low-risk passengers into a country, while providing a secure method for applicants, governments and airlines to verify acceptance for travel. The ICAO recommends that an ETS should integrate the pre-travel verification system with an interactive API system.[68] While the API Directive only calls for a batch-type data transfer, the future introduction of ETIAS and of EES calls for a consideration of an Interactive API.[69]

iAPI is an evolution of API where interactive queries are sent pre-departure to a national authority and receive a response indicating the likely border control status of the passenger. There are at least 18 iAPI implementations in operation around the world, with Australia, the United States (US), Canada, and the UK representing mature implementations.[70].

In the EU, if no other changes are made to API transmission following the introduction of the interactive query to ETIAS and EES (VIS), passenger data will be captured once but would require different transmissions: batch API data transfers to competent national authorities and an interactive query against the EES and ETIAS central systems (see Figure 2).

[67] Article 45(7) of the ETIAS Regulation.

[68] Evaluation of Council Directive 2004/82/EC of 29 April 2004 on the

Obligation of Carriers to Communicate Passenger Data, available at: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/policies/irregular-migration-return/return-readmission/docs/evaluation_of_the_api_tor_en.pdf, p.36

[69] Evaluation of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, available at: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/policies/irregular-migration-return/return-readmission/docs/evaluation_of_the_api_tor_en.pdf, p.36.

[70] Feasibility study on a centralised routing mechanism for advance passenger information (and passenger name records). Volume 1: main report - Publications Office of the EU (europa.eu).

Figure 2. ***API transmission in the baseline "+"***

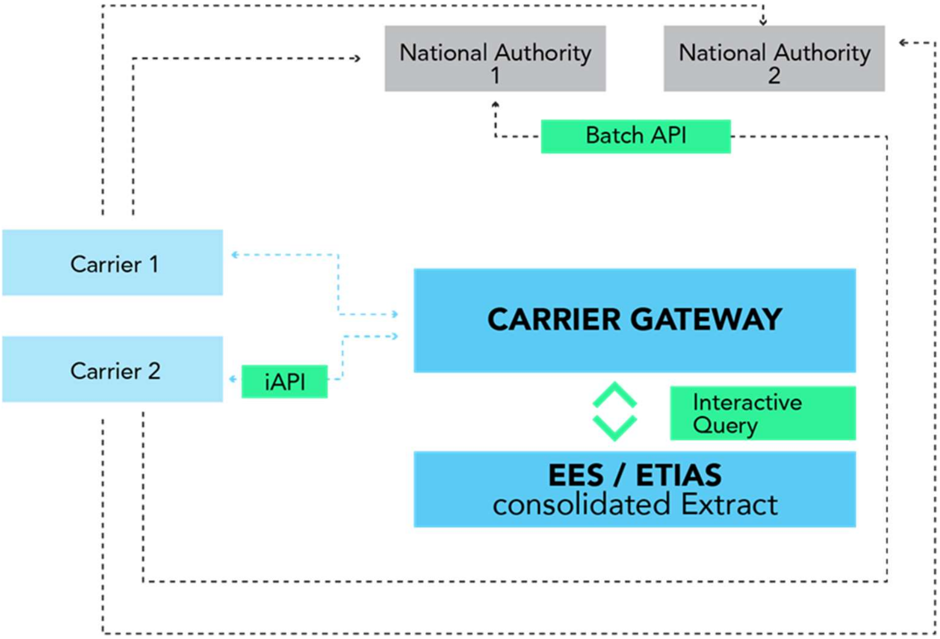


Table 6. Overview of passenger data requirements in API Directive compared to international standards, ETIAS, EES, VIS and SIS systems

Passenger data	API Directive	International standards		Other EU databases								
				Border management								
		MRZ	WCO /ICAO/ IATA Guide (PAXLST)	ETIAS (travel authorisation data)*	ETIAS (carrier gateway query)	EES visa holders (individual file)	EES visa-exempt (individual file)	EES visa holders (entry/exit record)	EES visa-exempt (entry/exit record)	EES (carriers)	VIS	SIS (borders)
Biographic data												
Full name	🟩										░	░
Surname (family name)/given name(s)		🟩	🟩	░	░	▓	▓			▓	░	░
Date of birth	🟩	🟩	🟩	░	░	▓	▓			▓	░	░
Place of birth			🟩	░							░	░
Nationality	🟩	🟩	🟩	░	░	▓	▓			▓	░	
Additional nationalities				░		▓	▓			▓	░	
Gender/sex		🟩	🟩	░	░	▓	▓			▓	░	░
Travel document data												
Travel document number	🟩	🟩	🟩	░	░	▓	▓			▓	░	░
Travel document type	🟩	🟩	🟩	░	░	▓	▓			▓	░	░
Issuing state or organisation of the official travel document		🟩	🟩	░	░	▓	▓			▓	░	░
Issue date of the travel document				░								
Expiration date of official travel document		🟩	🟩	░	░	▓	▓			▓	░	
Other document number used for travel			🟩									
Type of other document used for travel			🟩									
Visa number			🟩					▓			░	
Issue date of the visa			🟩								░	
Date of expiry of visa								▓			░	
Place of issuance of the visa			🟩					▓			░	
Additional passenger information												
Seating information			🟩									
Baggage information			🟩									
Traveller status			🟩									
PNR locator number			🟩									
Address of primary or permanent residence			🟩	░							░	░
Destination address			🟩	░							░	
Biometric data												
Facial image						▓	▓				░	░
Fingerprints							▓				░	░
Other data												
Date of entry								▓	▓	▓		
Time of entry								▓	▓	▓		
Border crossing point	🟩				Member State of entry			▓	▓	▓		
Authority that authorised entry								▓	▓	▓		
Status of third-country national								▓	▓	▓		

3.2.2 Use of passenger data for public health purposes

Border checks on a person entering the territory of a Member State include vetting whether or not the person poses a threat to public health[71].

A legal basis to check whether an applicant for travel authorisation poses a high epidemic risk is included in the ETIAS Regulation. 'High epidemic risk' is defined as '*any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization (WHO) or the European Centre for Disease Prevention and Control (ECDC) and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States'* (Article 3(1)8 of the ETIAS Regulation).

COVID-19 has had a significant impact on the business activity of carriers and on passenger travel[72]. The pandemic also raised the question of the possible collection of additional passenger information to improve traceability and support public health objectives.

Currently, passenger health data can be collected in two ways: **passenger health declaration forms** or **passenger locator forms (PLF)**. The former are implemented as part of the entry screening procedures and comprise a questionnaire exploring possible exposure to disease or other symptoms. Health declaration forms are distributed to passengers during a flight/upon arrival or filled out on a website/app before the flight. These were used and developed during the (ongoing) COVID-19 pandemic, with varying approaches. In some cases, air carriers had to distribute and collect these forms from passengers, while public health authorities were required to screen them and follow-up with passengers. However, processing information from paper-based forms created delays and inefficiencies in the screening process, and ran the risk of higher transmission of COVID-19[73]. Moving away from paper forms is considered to improve screening processes and data quality, with mobile apps envisaged to supplement and expedite the completion of the questionnaire.

A PLF was developed by ICAO and IATA since 2012. It aims to support public health authorities in carrying out contact tracing for passengers potentially exposed to a communicable disease during a flight or while travelling[74]. More specifically - and depending on the public health regulations in use in the country of arrival - passengers fill out a form in-flight which is later handed to either the aircraft crew or passport control. PLFs are different from passenger health declaration forms, which are developed in relation to a specific disease[75]. PLFs may include passenger name, gender, travel companions, contact details for tracing purposes (address of permanent residence, destination address, telephone numbers, email address) and travel history (destination address in the host country)[76]. As these forms were developed to cater for different situations, the ICAO and European Centre for Disease Prevention and Control (ECDC) recommend distinct health forms and PLFs.

[71] Article 6(1)(e) and Article 8(2)(b) of the Schengen Borders Code: 'threat to public health' means any disease with epidemic potential as defined by the International Health Regulations of the WHO and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.

[72] https://aviationbenefits.org/covid-19s-impact-on-air-transport/

[73] https://www.ecdc.europa.eu/sites/default/files/documents/ECDC-one-page_EntryScreening_Passenger-Locator-and-Health-Declarations.pdf

[74] https://www.ecdc.europa.eu/sites/default/files/documents/ECDC-one-page_EntryScreening_Passenger-Locator-and-Health-Declarations.pdf

[75] The ECDC advises passenger health declaration forms to be collected and processed by health professionals and stored in a separate database, as such forms contain sensitive personal health data.

[76] https://www.iata.org/contentassets/67e015cf3db1410392cd5b5bb5961a16/iata_collection-of-self-declared-passenger-health-data_version-3_9-june-2020.pdf; https://www.ecdc.europa.eu/sites/default/files/documents/ECDC-one-page_EntryScreening_Passenger-Locator-and-Health-Declarations.pdf

3.3 Problem definition

Three particular issues are evident in the current functioning of the API Directive at national level and across the EU.

Problem 1: Uneven scope of the collection and processing of API data across EU/Schengen Member States

The API Directive sets out a range of minimum requirements for Member States (e.g. the list of API data elements which can be requested, transmission modes, messaging protocols). This gives Member States the discretion to request additional data elements from different carriers and routes, in line with national legislation. This creates discrepancies in the requirements placed on air carriers, as well as a lack of a harmonised approach in the collection and processing of API data across the EU. Ultimately, this leads to uncertainty about the rules applicable to the collection and use of API data and security loopholes, as passenger information is not consistently collected and processed throughout the EU.

The main causes underpinning this problem are:

- ***Cause 1: The list of data elements provided in the API Directive is not exhaustive and does not reflect international standards***

The list of data elements provided in the API Directive concerning passenger and flight data is not a closed list. It is no longer aligned with the more detailed and closed list of data established by international guidelines and standards (IATA/WCO/ICAO API Implementing Guidelines, Annex 9 to the Convention on International Civil Aviation (Chicago Convention) and the PAXLST message standard), nor with the approach adopted by more recent EU instruments in the field of border management and law enforcement (e.g. PNR Directive, ETIAS and EES (VIS) Regulations).

- ***Cause 2: The scope of application of API-related obligations on carriers' routes, mode and type of passenger transport differs across Member States***

The API Directive obliges air carriers to transmit passenger data to the destination Member State prior to or shortly after take-off, if that flight is in-bound from a third country and at the request of the authorities responsible for carrying out checks on persons at external borders. The implementation of the Directive shows that while a majority of Member States collect API data for all-inbound extra-EU/Schengen flights, others collect data on selected flights only. Likewise, while a majority of Member States request API data from all air carriers, some request this data only for selected air carriers.

- ***Cause 3: API data are processed for different purposes***

The API Directive sets out an obligation to collect API data for border control purposes. The use of such data for law enforcement purposes is, however, left to the discretion of Member States, without providing a clearer definition of this objective (type of crime and offences, as per the PNR Directive). This has led to Member States adopting different practices with regard to the purpose of processing API data. More recently, Member States implemented changes to their national legislation (including provisions regulating API data) with the transposition of the PNR Directive in mind. This created additional inconsistencies in the framework applicable to the transmission and processing of API data.

Problem 2: Organisational, operational and technological means for capturing, transmitting and processing API data are not harmonised

From an organisational perspective, the API Directive does not mandate specific organisational structures or responsible authorities (except for authorities responsible for border controls) to perform the obligations set out. This creates an administrative burden for carriers as they need to understand each national organisational model to transmit API data to the relevant national – and in some cases sub-national – authorities in each implementing Member State.

API data is most useful when 'verified', and issues with accuracy or completeness of data transmitted by carriers impact the efficiency of API data collection and processing. The operational procedures for capturing, transmitting, processing and analysing API data vary in their methods, timing, format and frequency of transmission across implementing Member States.

The main causes underpinning this problem are:

- ***Cause 1: The list of API data elements provided in the Directive is not exhaustive and does not reflect international standards***
  See above.

- ***Cause 2: The methods used to collect, verify and transmit data, as well as their timing, differ between Member States***

The format and time taken to collect and transmit the data, as well as methods to verify data, are not specified in the API Directive. As regards transmission time, the Directive provides that API data are to be transmitted 'by the end of check-in', giving Member States the option to request the transmission of API data several times (e.g. even after formal closure of check-in). While data are typically captured by air carriers from the MRZ, the current legal framework does not allow national authorities to impose the mode of API data collection on carriers, nor does the current framework refer to internationally agreed standards. The different requirements implemented by Member States in respect of the methods used to collect, verify and transmit data result in situations where carriers have to adapt to a variety of requirements from several Member States. This creates the potential for errors or instances where the API data message is wrongly formatted or not transmitted on time to the national authorities. Eventually, this can prove a source of additional cost and legal uncertainty.

Problem 3: Current API implementation is not fully interoperable with other EU information systems in the fields of border management and law enforcement

Since its adoption in 2004, the API landscape has evolved significantly. Several border management instruments, such as Regulation 2017/458 on the reinforcement of checks against relevant databases at external borders, refer to the use of API data. The implementation of the ETIAS and EES (and VIS) systems will also require carriers to query these systems with similar passenger data.

The main causes underpinning this problem are:

- ***Cause 1: The list of API data elements provided in the Directive is not exhaustive and does not reflect international standards***
  See above.

- ***Cause 2: The scope of application of API related obligations on carriers' routes, mode and type of passenger transport differs between Member States***
  See above.

These three main problems impact API data collection and processing across the EU, generating a certain level of legal uncertainty, for the entities collecting and transmitting the data, for the authorities processing those data, and, ultimately, for travellers.

As the Directive is not entirely prescriptive on the data elements, time of transmission or format of messages, varying API data collection requirements across Member States are a great source of legal uncertainty for carriers and a source of incoherence in implementation of the Directive. The possibility in the API Directive to request API data for law enforcement purposes created inconsistencies in respect of the transmission of

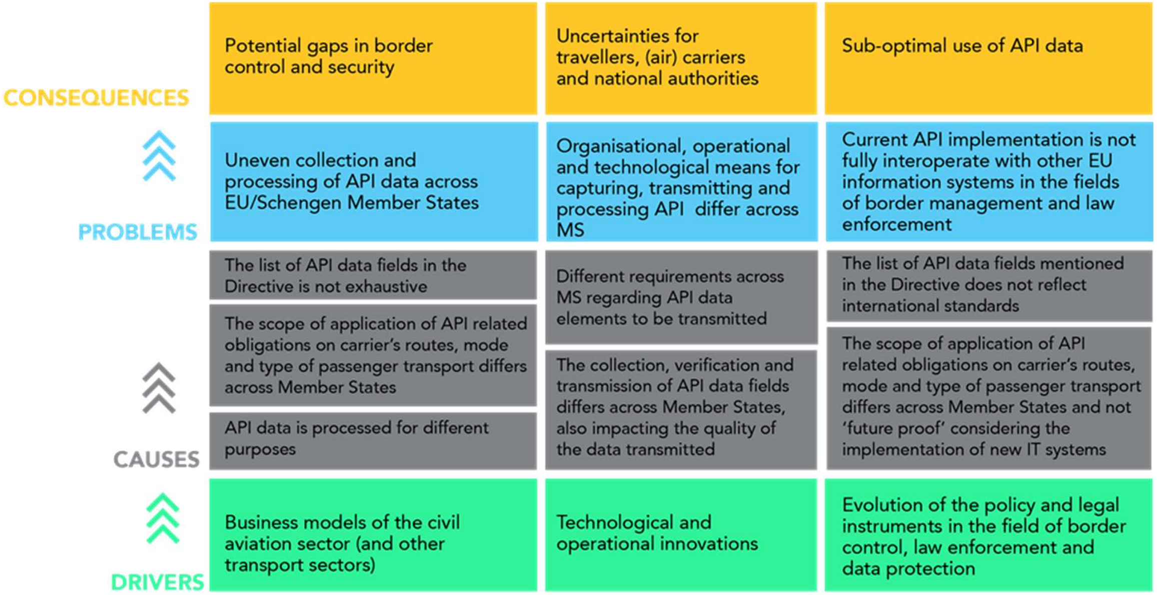
API data to national authorities. This is because the mandated data elements in the API and PNR Directives do not entirely correspond with one another (e.g. requirements are not applicable to the same types of flights or to different geographies).

The current situation whereby API data is collected for specific types of flights and certain routes or categories of air carriers may result in inconsistent collection, processing and use of API data. This may create a gap in both border management controls and law enforcement in the EU. These inconsistencies may create security loopholes, as gaps in coverage can be exploited by serious and organised crime organisations or terrorist organisations adapting their modus operandi to the existence of obligations to collect passenger data on specific transport modes.

The API Directive explicitly refers to air carriers for which API data should be collected but does not exclude its application to other transport modes based on national law. Some Member States' national legislation requires the collection of API data for other modes of transport (maritime carriers, rail, coaches), as a representative share of passengers enter their territories through modes other than air. A lack of API data collection on sea and land may potentially create an information gap from a border control and security perspective, as well as in light of the future implementation of ETIAS and EES.

Inconsistent implementation of the current API framework leads to sub-optimal use and processing of API data. This is due to the misalignment of data fields mandated in the API Directive with more recent EU systems in the area of border controls and law enforcement. Data quality issues hinder full exploitation of API data by national authorities. The current multiple requirements on carriers to transmit similar API data through several messages to different national authorities create unnecessary technical and operational burdens.

Figure 3. ***Problem tree supporting possible measures on API***



CONSEQUENCES	Potential gaps in border control and security	Uncertainties for travellers, (air) carriers and national authorities	Sub-optimal use of API data
PROBLEMS	Uneven collection and processing of API data across EU/Schengen Member States	Organisational, operational and technological means for capturing, transmitting and processing API differ across MS	Current API implementation is not fully interoperate with other EU information systems in the fields of border management and law enforcement
CAUSES	The list of API data fields in the Directive is not exhaustive The scope of application of API related obligations on carrier's routes, mode and type of passenger transport differs across Member States API data is processed for different purposes	Different requirements across MS regarding API data elements to be transmitted The collection, verification and transmission of API data fields differs across Member States, also impacting the quality of the data transmitted	The list of API data fields mentioned in the Directive does not reflect international standards The scope of application of API related obligations on carrier's routes, mode and type of passenger transport differs across Member States and not 'future proof' considering the implementation of new IT systems
DRIVERS	Business models of the civil aviation sector (and other transport sectors)	Technological and operational innovations	Evolution of the policy and legal instruments in the field of border control, law enforcement and data protection

3.4 Policy option I: Possible measures on the scope of API data fields

This option examines the type of mandatory and additional API data fields for carriers to transmit to border management and/or law enforcement authorities. The assessment of the policy option covers the added value of a closed and mandatory list of API data fields, which are necessary for both migration management and law enforcement purposes. The first scenario examines the scope of API data fields for border and migration management purposes, while the second examines the law enforcement purpose. Additional API data fields are considered in light of agreed international standards, as well as the technical and operational implications for carriers to transmit additional API data.

3.4.1 Assessment of the baseline

Member States implemented their API systems to pursue several objectives, ranging from improving border control and combating irregular migration, to law enforcement. While the API Directive is primarily used for migration management, Member States also process API data for the purposes of enhancing internal security and public order, fighting terrorism and ensuring national security[77]. However, the API Directive does not expand on the data fields that can be processed for law enforcement purposes, unlike the PNR Directive, which contains a list of serious offences and crimes for which PNR data can be processed. This situation leads to diverging processing practices across the EU.

API data fields are effective[78] in supporting national authorities (border management authorities) to identify fraudulent documents, identify high-risk passengers, detect and prevent irregular migration, and provide necessary information to cross-check passenger data against information contained in other databases (EU and national databases) before their arrival at the border check (first-line checks), as well as in-depth checks (second-line checks).

The list of data elements included in the API Directive is non-exhaustive and Member States can request additional data elements in line with national legislation (see section 3.1). All stakeholder types pointed out that the lack of alignment of API data elements with international standards creates a gap and is an obstacle to the Directive's effectiveness. Among the data fields considered necessary for advance screening of passengers, fields such as are gender, the issuing State or organisation of the official travel document, and expiry date of the travel document validity. The latter are data elements contained in the MRZ but not included in the API Directive. Seat and baggage information were also reported as necessary in the fight against irregular migration and customs control, as well as for health. The absence of API data on cabin crew members was highlighted as a possible factor limiting the effectiveness of the API Directive. The PNR locator that can be included in the API message is valuable in allowing authorities to reconcile the information sent as part of the API and the PNR message.

In addition to the data fields listed in the API Directive, most Member States request the collection of data fields contained in the MRZ for border control purposes (surname/given names, date of birth, nationality, gender, travel document number and type, issuing state or organisation, expiry date of the travel document)[79]. In several Member States, this practice dates back to the implementation of the API Directive in 2006. In addition to the flight data elements listed in the API Directive (border crossing point of entry, code of transport, departure and arrival time, initial point of embarkation), the majority of Member States collect information on the scheduled

[77] 2020 evaluation.

[78] See Annex 7 for results of the border management authorities' survey.

[79] See Annex 7 for results of the border management authorities' survey.

departure and arrival date, as this is aligned with the WCO/ICAO standard used as a reference by most States.

API data are included under Annex I, point 18, of the PNR Directive which lists data elements additional to those listed in Article 3(2) of the API Directive. These include gender, departure and arrival date of transportation, name of the airline, flight number, country of issuance, and expiry date of the travel document. Information on flight identification, gender, country of issuance and expiry date of the travel document are often collected by law enforcement authorities. Seating and baggage information are collected by six Member States[80].

The retention of API data for 24 hours for border control purposes was not consistently implemented in all Member States, in part due to the changes in the organisational set-up and implementation of the PNR Directive (Single Window). As a result, the 24-hour limit set out in the API Directive was deleted from national legislation in some Member States, creating either a legal grey area on the retention requirements applicable or leading to the sole application of the requirements set out in the PNR Directive, despite the fact that API data and PNR data are different and are processed for different purposes.

Table 7 below gives an overview of the assessment of this baseline using a scoring tool.

Table 7. Overview of the assessment for policy option I, scenario 0

Policy option I, scenario 0			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	■■■□□
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at EU external borders	■■■□□
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	■■■□□
	Auxiliary objective	Public health control	□□□□□
Overall effectiveness assessment			■■■□□
Efficiency	***Costs***	Carriers	■■■■□
		Border management authorities	■■■□□
		Law enforcement authorities	■■■□□
	Benefits	Better passenger data	■■□□□
		Better risk analysis	■■■□□
		Better operational planning	■■■□□
		Better operational response	■■■□□
Overall efficiency assessment			■■■□□
Coherence	Streamline API with international standards		■■□□□
	Objectives of the Schengen Borders Code		■■■□□
	Objectives of EES Regulation		■■■□□

[80] Seating information: BE, CZ, DK, FR, RO, SK; baggage information: BE, DK, HU, FR, RO, SK.

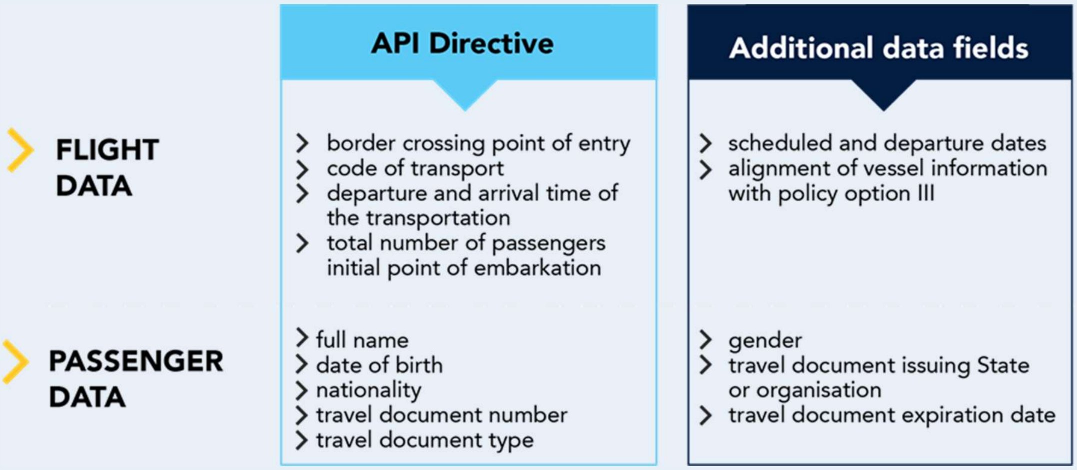
	Objectives of ETIAS Regulation	■■■□□
	Objectives of VIS Regulation (and proposed recast)	N/A
	Objectives of the Interoperability Regulation	N/A
	PNR Directive objectives	■■□□□
Overall coherence assessment		■■□□□
Overall data protection and fundamental rights assessment		■■□□□

3.4.2 Policy option I, scenario 1: List of API data fields for border and migration management purposes

Summary of scenario 1

- This scenario considers the type of data fields to be collected for border and migration management purposes. It proposes a closed and mandatory list of passenger information to enhance harmonisation and implementation across EU Member States. It would align future API data elements with MRZ fields (and thus with ICAO's PAXLST standards) and categorise data fields according to their availability and necessity for border and migration management purposes.
- In addition to the passenger information already listed in the API Directive, this scenario mandates the collection of the following additional fields: **gender, the issuing State or organisation, and the expiry date of the official document.**
- In addition to the flight information listed in the API Directive, this scenario obliges the inclusion of **scheduled and departure dates** as additional fields. It also considers changes to the formulation of flight information should the scope of application of the Directive be extended to other transport modes (i.e. formulation of vehicle registration and points of origin and destination).
- This scenario includes the extension of the personal scope of application of the API Directive, namely collection of both passenger and **crew data**.
- This scenario considers the possibility for national authorities to request API data from **commercial passenger flights** only (the implications of extending this type of requirement to charter flights, cargo and business aviation is assessed in policy option II).
- Finally, this scenario considers the processing of API data for **public health purposes**.

Figure 4. Additional data fields in policy option I, scenario 1



API Directive

Additional data fields

FLIGHT DATA

API Directive:
- border crossing point of entry
- code of transport
- departure and arrival time of the transportation
- total number of passengers initial point of embarkation

Additional data fields:
- scheduled and departure dates
- alignment of vessel information with policy option III

PASSENGER DATA

API Directive:
- full name
- date of birth
- nationality
- travel document number
- travel document type

Additional data fields:
- gender
- travel document issuing State or organisation
- travel document expiration date

3.4.2.1 MCA: assessment of effectiveness

Under this scenario, border and migration management remains the main purpose of future legislation on API, with data primarily used for the identification of travellers and to increase the quality of the identification process at external borders.

Access to competent authorities such as customs authorities is not prohibited by the current formulation of the API Directive. The approach of providing access to competent authorities involved in border management should be continued in future legislation to preserve each Member State's institutional and administrative autonomy (i.e. sticking to the missions of competent authorities rather than their specific name or function). When performing border control missions, customs authorities generally have direct access to the national API system, in keeping with other border control authorities.

The existing list of API data fields is not fully adequate to ensure the effectiveness of (advance) border controls because a number of fields that would be useful necessary to authorities (which this policy option seeks to introduce) are not mandated by the current API Directive. The missing data elements relate to gender, issuing State or organisation, and expiry date of the official travel document. Data related to biographical information in the API data elements listed in a future instrument (contained in the travel document) should be limited to the eight data elements of the MRZ of a travel document. A mandatory list of API data following the fields covered by the MRZ would ensure consistency in the data collected from passengers throughout their passenger journey and matches performed with other databases checked during border control (ETIAS, EES, SIS, etc.).

A closed and mandatory list would bring legal certainty and increased standardisation in the collection, transmission and use of API data throughout the EU.

As per international standards, States have the option to request API crew data, which are already collected by air carriers. When required, crew data are transmitted to Member States through a separate batch crew PAXLST message, which contains an element to identify it as a crew message. Data collected on crew members would amount to the same data fields as passengers. This would include, for instance, the full name, gender, date of birth, nationality, country of residence, address of permanent residence, passport number and country of issuance and expiration date, in addition to pilot certificate number, country of issuance, and status onboard the aircraft/ crew position. This would also help with the integration of data collected from crew members in the maritime sector (see Table 6). Although crew are exempt from ETIAS/EES requirements, they are subject to specific border checks[81]. Prior to obtaining crew status, the standard security checks focus on terrorism and other serious crime and not on the risk of irregular migration. Therefore, from a border management perspective, cases of irregular migration among crew members also warrant the collection of their data.

Scheduled flight departure and arrival data would complete current departure and arrival times. This would align with international standards and practices and also support the reconciliation of planned versus actual departure and arrival times.

Extending the scope to other transport modes in policy option III would entail the mandatory collection of **additional vessel/route information** (e.g. vessel identification or equivalent, wagon or cabin number, port of departure and arrival) and thus would require reformulation of data fields in a more inclusive way to accommodate other modes of transport.

In light of COVID-19, including an auxiliary purpose authorising the processing of API data for public health purposes would future-proof API legislation should a similar

[81] As per Article 2.2 (i) of the ETIAS Regulation, referring to points a) to f), Article 4, Regulation 539/2001 (exemptions for air and sea crew) and per Article 2.3 (g) of the EES Regulation, referring to Article 6a(3) point (g) of Regulation (EU) 2016/399 (amended by Regulation 2017/2225).

situation arise in the future. Envisaged first as a border control instrument, adding this purpose explicitly in the legal basis would merely act as a reminder of current practice. Indeed, border checks on a person entering the territory of a Member State include vetting whether or not the person poses a threat to public health[82]. This would also align API legislation with the ETIAS Regulation, which contains the legal basis to check whether an applicant for a travel authorisation poses a high epidemic risk[83].

There is no need for additional data fields to be added specifically for public health purposes in the API message, but rather to allow access to the identification data that

Discarded data elements for border control purposes

The following data elements were also mentioned during stakeholder consultations as additional fields that could be somewhat which, to some extent, could be useful for border and migration management purposes:

- **Place or country of birth:** to enhance passenger identification and reduce false positives and support the risk assessment in second- line checks. This data element can also be found in the SIS (borders), VIS, and the travel authorisation application stored in ETIAS.
- **Destination address**: to support the assessment of a passenger in a first-line and second-line checks; to support decision-making as to whether a passenger fulfils the requirements to enter the Schengen -area; and to support risk analysis for detecting irregular migration. Destination addresses for a certain category of third-country nationals can be found in VIS and in the travel authorisation application stored in ETIAS.
- **Address of primary or permanent residence:** to support a more effective passenger identification at the external borders. This data element is also stored in the SIS (borders), VIS and the travel authorisation application stored in ETIAS.
- **Visa data** (such as the visa number, issue date, place of issuance): information relevant to assess cases of irregular migration, confirm validity of travel documents, and fight against document fraud. Information on short-term Schengen visas is stored in VIS.
- **Type and number of other document(s) used for travel**: to support first-line and second-line checks in other databases (e.g. cases of double check-ins by the same person using different travel documents).

The above listed data elements are not normally found in airline systems and, therefore, if requested, are non-verifiable nor non-validated data. Ultimately, the data quality requirements would not apply in the same way for these types of data compared to MRZ data fields. Information related to addresses are purely declarative data that and must be collected manually. Secondary travel documents issued in the EU include an MRZ.; However, those issued in other third-countries may not have an MRZ and therefore would need to be manually captured. T; there is also a lack of standards to capture this information in the PAXLST message.

Additionally, information on the destination address and address of primary/ or permanent residence of third-country nationals subject to a visa requirement is also stored in ETIAS and VIS. As regards visa data, in the context of implementation of the EES, border checks on entry and exit from the Schengen area will also include checks in VIS. National authorities generally use the travel document number and nominal data to perform automated checks against a number of databases, including SIS, VIS and other national databases containing for instance information on national (long-term) visas and residence permits (national authorities own this information).

[82] Article 6(1)(e) and Article 8(2)(b) of the Schengen Borders Code: 'threat to public health' means any disease with epidemic potential as defined by the International Health Regulations of the WHO and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.

[83] 'High epidemic risk' is defined as "*any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization (WHO) or the European Centre for Disease Prevention and Control (ECDC) and other infectious diseases or contagious Disease Prevention and Control (ECDC) and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States*" (Article 3(1)8 of the ETIAS Regulation).

API provides and that could be relevant for competent national authorities dealing with public health emergencies. This would also preserve the main purpose of API data - border management - and safeguard a clear framework around its processing as identification data and not potential health data. The latter is a specific category of personal data, subject to specific measures and safeguards, as per EU data protection rules[84], following a different stream and channels of transmission and processing rules.

3.4.2.2 MCA: assessment of efficiency

Costs

The impacts on costs for carriers are limited where additional data elements are within existing and standardised MRZ fields.

The implementation of this scenario would have limited technological and operational implications for commercial air carriers: the list of API data is aligned with data corresponding to MRZ and already available in (most) of the commercial airlines systems (Departure Control Systems or other systems). Industry stakeholders noted that any additional data element required outside of the MRZ would impact the check-in and boarding processes (additional time), as it would require manual collection. Adding data outside the MRZ data fields would also imply an adaptation of the check-in systems (mobile, web or kiosk), which would take approximatively six months to implement.

Likewise, the infrastructure and maintenance costs for the transmission of API messages should remain quite similar (if no changes to the current situation).

These costs could slightly increase with the transmission of the API crew message. It is already widespread in practice to collect crew information for airlines' operations. The PAXLST standard applies both to passengers and crew.

In relation to the transmission of the API crew message, crew composition may change up to the last moment before take-off, thus common international practice is for States to only require crew API at the time of flight closure (and not before) in order to guarantee full accuracy of the information.

Volume of crew members can also impact on carriers' costs. However, this is largely a standard practice across industry and volumes of crew members are significantly lower than numbers of passengers (crew members constitute 1-4% of passenger load onto a plane).

Operational and technical impacts on border management authorities would be limited to the modification of national API systems and operational guidelines, with little need for organisational change or staff training. Consultations confirmed that additional data fields would generally not affect the API data processing time per passenger. In those Member States where this scenario would represent additional data elements, it could impact the processing time per passenger.

The calculated costs across the relevant stakeholder groups are shown below (see Annex 6 for the full methodology used for the calculation of costs).

[84] Article 9(2)(i)) of the GDPR provides that the processing of personal health data is prohibited except where this processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

Table 8. Overview of costs across stakeholder groups

Stakeholder	**Estimated additional costs** (rounded to the nearest million) ***Scenario 1***
Air carriers	EUR 215.0 million
Border management authorities	EUR 3.0 million
Law enforcement authorities	Not applicable

Source: ICF estimates

Benefits

Compared to the current situation, a set of closed and mandatory data fields would have tangible benefits in harmonising API requirements across all EU Member States. A single set of data would simplify the transmission requirements for industry stakeholders and increase certainty. Several stakeholders suggested that a Regulation would be a more appropriate legal instrument rather than a recast Directive. A Regulation would facilitate the implementation of a 'closed list' of API data throughout the EU and limit the discretion of Member States to request additional data fields, which would eventually contribute to more unified processing of API data. However, this would also imply that national authorities would not be allowed to collect other data fields outside those listed in this scenario and potentially change national legislation.

The additional data fields on gender, the issuing State or organisation, and the expiry date of the travel document would bring API legislation in line with current practices, whereby this information is necessary for the identification of a passenger (and crew member). Ultimately, this would better support border management authorities to carry out inspections and controls in respect of specific passengers through advance screening of their API data.

Collecting API data on crew would close the operational security gap highlighted by stakeholders at EU and national level. Checks at the borders include cross-checking against flagged persons in either national watchlists or alerts in other databases. As information on crew does not reach border guards together with passenger information, the identity of crew members placed on that list escape control (at the first border control check).

Additional API data would not negatively impact travellers' experiences. Where API data elements are limited to MRZ elements, this amounts to presenting the data already contained in the travel document.

This scenario also limits the concerns related to data protection: the data included in the MRZ is generally considered the data to which border guards have access when looking at passengers' travel documents. Collecting additional data that are not already accessible to the border guard might generate more data protection concerns.

3.4.2.3 MCA: assessment of coherence

This scenario brings stronger coherence and alignment of requirements at EU level with international standards and practices.

From carriers' perspectives, this scenario would also ensure further standardisation and consistency with future requirements under the ETIAS. To query ETIAS, they will have to submit data contained in the MRZ, as well as indicate the Member State of entry[85].

[85] Article 45(2) of the ETIAS Regulation.

From national authorities'/end-users perspectives, better and more reliable passenger data would facilitate the verification of the identity of persons whose data are stored in different IT borders and visa systems. Complete travel document data would support the detection of fraudulent identity when comparing with data stored in another system.

3.4.2.4 MCA: assessment of data protection and fundamental rights

The fundamental rights affected by this scenario are primarily the right to privacy (Article 7 Charter of Fundamental Rights) and the right to personal data protection (Article 8 of the Charter of Fundamental Rights). This scenario would impact these rights, as the data processing would entail additional data elements. However, there would be no change to the modes of data collection and transmission or to the authorities using the data. Given that, the majority of Member States already collect such data as per the MRZ and international standards (the API Directive does not provide for a closed data list), in practice, mandating the fields to align to MRZ, would have only a minor impact on the right to privacy, yet to a limited extent, as the data elements include small amounts of data that would give information on a passenger's private life. The right to personal data protection would also be impacted to a limited extent, as this scenario does not entail additional data processing to the baseline.

Constraining data collection to the MRZ dataset is a minor limitation on the right to data protection and is limited to what is strictly necessary for identity and travel document checks at the border. The data elements covered in this scenario do not include special categories of data that can be considered particularly sensitive (e.g. biometric data, health data). Additionally, processing of data in the MRZ will guarantee better quality data, reinforcing the accuracy of data matches in databases and reducing false positives.

As per the analysis carried out for the 2020 evaluation, the processing of personal data for border management purposes falls under the framework of the GDPR. The aim of the scenario is to bring the current provisions on data protection in line with the latest GDPR framework (e.g. oversight mechanism, ways to inform passengers, available remedies in case of breaches). It would thus not affect the possibility of passengers to seek remedies or access to information stored (in national API systems) but, rather, strengthen such procedural safeguards.

The data retention period under this scenario is contingent on the purposes and policy objectives of the data processing. In this scenario, there are two relevant sub-objectives. Firstly, where the processing of API data is mandated for border checks, there is no need to retain data longer than necessary to carry out border checks and data can thus be deleted by carriers after transmission and by competent authorities after completing the check. The current 24-hour limitation responds to this purpose or sub-objective. However, national authorities consulted for this Study highlighted instances where receiving data 24 hours in advance was not enough to prepare for border checks, in particular for routes and travel connections which take longer than 24 hours. Stakeholders thus suggested extending the data retention to 48 hours.

Secondly, migration authorities and border authorities are entrusted with additional missions, such as risk analysis and second-line checks on travel documents to detect document fraud or irregular migration (e.g. processing API data to trace the travel history of a person). There would be a need for a longer data retention period to achieve this purpose or sub-objective (irregular migration). Longer retention of data would support border guards to better identify persons who may pose a risk.

Measures mandated in this scenario are proportionate to the impact on fundamental rights (data protection and privacy) and the list of additional data fields is proportionate to the objectives pursued. Only data that are relevant for border checks and irregular migration would be collected and processed, namely biographical and travel document data. The data elements listed here do not go beyond what a border guard already sees when examining travel documents (e.g. those contained in the MRZ). Any risks of unlawful access or use of the data would be mitigated by the existing technical and security features implemented by existing API systems.

With respect to fundamental rights and data protection, the limitations brought by this scenario are assessed as justified and proportionate to the objectives pursued.

Table 8 summarises the MCA for policy option I, scenario 1.

Table 9. Overview of assessment for policy option I, scenario 1

Policy option I, scenario 1			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■□□□
		Enhance the security of citizens in the EU	N/A
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at the EU external borders	■■■□□
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	N/A
	Auxiliary objective	Public health control	■■■□□
Overall effectiveness assessment			🟦🟦🟦□□
Efficiency	***Costs to…***	Carriers	■■■□□
		Border management authorities	■■□□□
		Law enforcement authorities	N/A
	Benefits	Better passenger data	■■■□□
		Better risk analysis	■■■□□
		Better operational planning	■■■□□
		Better operational response	■■■□□
Overall efficiency assessment			🟦🟦🟦□□
Coherence		Streamline API with international standards	■■■□□
		Objectives of the Schengen Borders Code	■■■□□
		Objectives of EES Regulation	■■■□□
		Objectives of ETIAS Regulation	■■■□□
		Objectives of VIS Regulation (and proposed recast)	■■■□□
		Objectives of Interoperability Regulation	■■■□□
		PNR Directive objectives	■■■□□
Overall coherence assessment			🟦🟦🟦□□
Overall data protection and fundamental rights assessment			🟦🟦🟦🟦□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

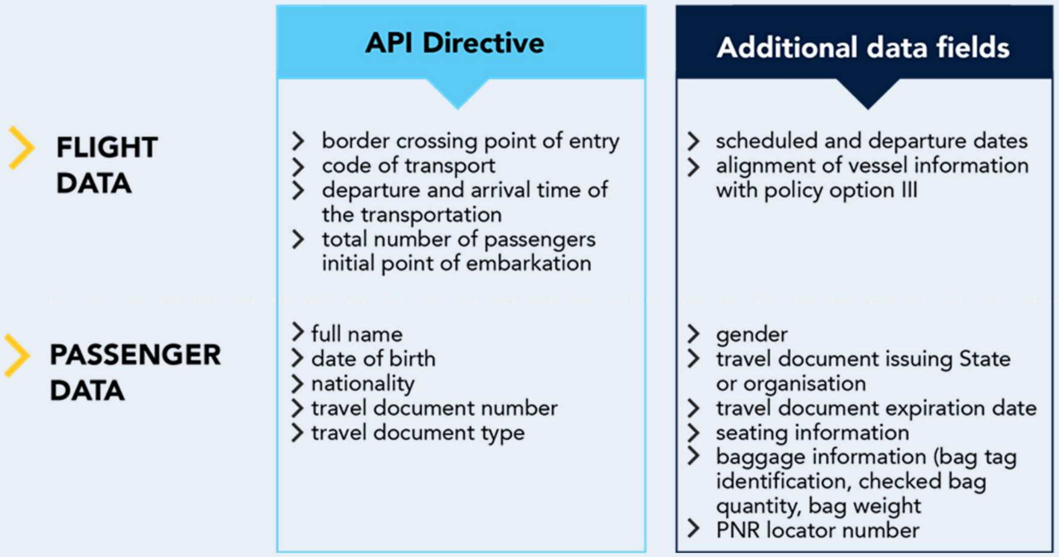
🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.4.3 Policy option I, scenario 2: List of API data fields for law enforcement purposes

Summary of scenario 2

- This scenario assesses the processing of API data for law enforcement purposes. As a first step, this entails **clarifying the purpose** in terms of offences for which data would be processed, as the current formulation of the API Directive led to divergent implementing practices across the EU. This approach is no longer aligned with that of more recent EU instruments on the processing of passenger data, which include a list of offences.
- As in scenario 1, this scenario mandates the collection of the following data fields in addition to those listed in the API Directive and the mandatory data elements listed in scenario 1:
    - **seating information;**
    - **baggage information** (i.e. bag tag identification, checked bag quantity and weight);
    - **PNR locator number.**
- Similarly, this scenario also mandates the collection and processing of **crew** (biographical) **data** by competent national authorities.
- This scenario also considers the **standardisation of protocols and data formats** to be used by carriers for the transmission of API data to national authorities and could take the form of an implementing decision attached to a future API instrument. Carriers may still transmit API data using 'old' versions of the PAXLST message, which does not contain baggage information fields, for example.

Figure 5. Additional data elements in policy option I, scenario 2



	API Directive	Additional data fields
FLIGHT DATA	› border crossing point of entry › code of transport › departure and arrival time of the transportation › total number of passengers initial point of embarkation	› scheduled and departure dates › alignment of vessel information with policy option III
PASSENGER DATA	› full name › date of birth › nationality › travel document number › travel document type	› gender › travel document issuing State or organisation › travel document expiration date › seating information › baggage information (bag tag identification, checked bag quantity, bag weight › PNR locator number

3.4.3.1 MCA: assessment of effectiveness

This scenario proposes an additional purpose for a future API instrument – the current provisions of the API Directive allow the possibility for Member States to collect and process API data for purposes other than border management. While law enforcement would not be the primary purpose in this scenario, the purpose(s) of data collection would be more clearly stated to ensure a level playing field and better stakeholder understanding of the aims of API data collection and processing. This would align with the approach adopted in the PNR Directive. For instance, clarifications could comprise the exact purpose of the use of data by national authorities in an annex, namely for preventing, detecting, investigating and/or prosecuting terrorism and serious crimes, with additional references to relevant EU legislation. In EU law, terrorist offences are defined by Directive 2017/541 and a list of serious crimes is included in Annex II to the PNR Directive. However, the latter adopts a narrower definition than other EU legislation, such as the European Arrest Warrant (EAW)[86].

The aim of this scenario is to allow competent authorities to directly receive and process API data for law enforcement purposes. API data could thus be used for more accurate watchlist matching through verified biographical data. PNR data is unverified information collected at the time of booking and is generally used for risk-based targeting. Due to the limitation of some airlines' systems, law enforcement authorities are not able to collect seat and baggage information from the PNR message sent by many airlines operating in Europe. Receiving a more complete API message would close this gap in PNR data collection.

Consultations carried out for this Study showed a consensus among stakeholders that the extra data fields (additional to the existing list in the API Directive and to elements listed in scenario 1) that would most enhance the effectiveness of the risk analysis conducted in combination with PNR data are seating and baggage information (i.e. bag tag identification, checked bag quantity and weight).

The combination of biographical data and seating and/or baggage information would reinforce the identification of suspects for certain crimes, such as trafficking in human beings, smuggling and organised crime (e.g. drugs). It could check whether the baggage weight is congruent with the purpose of the journey, while the baggage number could allow checks before the baggage is handed to the passenger at the collection point. These fields would allow law enforcement units to better analyse connections between suspects travelling on air routes or to narrow the entire passenger list to a minimum number of suspects.

The PNR locator number supports the matching of PNR and API data for an individual or booking.

Collecting crew data (identity and travel document details) is equally relevant for law enforcement missions, as this type of traveller is potentially involved in serious crime or terrorist offences. While exact numbers of suspected crew members were not found in the course of this research, stakeholder consultations revealed cases of crew members involved in 'continuous offences' (i.e. committed over a long period of time), where identification data would have supported earlier prevention of such crimes. Crew information could help competent authorities to identify patterns of fraud and the structure of organised crime.

[86] Council Framework Decision 2002/584/JHA. An EAW applies to all types of criminal offences and may be issued by a national judicial authority if the sought-after person is accused of an offence for which the maximum penalty is at least one year of prison or if they have been sentenced to a prison term of at least four months.

Discarded data elements for law enforcement purposes

Mirroring the list in scenario 1, data elements such as the **place or the country of birth**, **destination address** and **address of primary/ or permanent residence,** as well as **visa data** and **other travel documents** details were discarded. The availability of such data elements is not mandatory in the PNR Directive and consultations with national authorities explained the operational benefits of these elements for the identification of suspects in terrorism or other serious crime (e.g. such as drug trafficking). Place of birth or address is often the only intelligence competent authorities have to assess the risks posed by passengers. A similar assessment to scenario 1 can be applied in this scenario here: mandating the collection of this data elements as part of an API message would not achieve the necessary results in terms of the quality of data (data elements collected manually by airlines). Additionally, from a data protection perspective, such data elements are also accessible to law enforcement authorities (for some categories of passengers) in other databases (SIS police, VIS, ETIAS).

3.4.3.2 MCA: assessment of efficiency

Costs

Seating information and baggage information (i.e. bag tag identification, checked bag quantity and weight) are part of PAXLST standard and PNRGOV[87] standard but depending on airlines' systems, can be stored in different systems. Depending on their system set-up, airlines would be able to send seating and baggage information either as part of the PNR message (extracted from their reservation system) or as part of the PAXLST message (if the information is only stored in the DCS).

Airlines that already have the capability to include seating and baggage information in their PNR message should incur no additional costs. Airlines who can only include this information in the PAXLST extracted from their DCS (or from other systems) would have to upgrade their systems to support the latest PAXLST message formats.

This may vary within the same airline, depending on the system configurations they use at different destinations. Thus, the transmission of baggage information within the API message might incur additional costs for some smaller airlines in cases where it cannot be integrated in the existing DCS or reservation system. This could be solved with transmission of that information via a separate message.

Seating and baggage information could be incorporated within the PAXLST message, however this is possible only when airlines and authorities have the technical capacity to process PAXLST message version 05b (or greater) or 12b respectively (i.e. 2003 PAXLST version or later). If lower versions are being handled either by the airline or the authority, or the airline does not have the capability to include the conditional data elements (bag or seat) in the PAXLST, the transmission of this information might have to be done via a separate message[88]. Alternatively, or additionally, protocols and data formats could be harmonised by indicating the relevant (and newer) PAXLST message version to be used (i.e. update the version mentioned in PNR Implementing Decision[89]).

As the list of API data for border management purposes is different from that for law enforcement purposes, national authorities would need to set up a system to filter information on seating and baggage from the PAXLST message to border management authorities.

[87] PNRGOV is a messaging standard of Passenger Name Record (PNR), regulating how airlines and tour operators should manage and provide PNR data to PIUs.

[88] Considering policy option V, the carrier gateway can also translate the API data to an EU interoperable format, and leave the details of the carrier API data formats to the carrier gateway to manage.

[89] https://eur-lex.europa.eu/eli/dec_impl/2017/759

Carriers will have the obligation to send only one message, with all fields mentioned in scenarios 1 and 2.

For national authorities, more API data fields would mean that more risk profiles can be created, and the need for targeting and exchange of information (national and international level) will also be higher. Such changes may require additional personnel and tailored training.

The calculated costs across the relevant stakeholder groups are outlined below. The full methodology used for the calculation of costs is provided in Annex 6. It is worth noting that, compared to Scenario 1, it is expected that there will be some form of economies of scale for carriers under Scenario 2.

Table 10. Overview of estimated costs per stakeholder

Stakeholder	**Estimated additional costs (rounded to the nearest million)** ***Scenario 2***
Air carriers	EUR 103.0 million
Border management authorities	Not applicable
Law enforcement authorities	EUR 3.0 million

Source: ICF estimates

Benefits

Baggage and seating information is particularly relevant to detecting trafficking in human beings and smuggling, and in unravelling organised crime networks. The latter avoid purchasing tickets for groups (under the same reservation code), instead asking for seats next to each other at check-in. Seating information thus enables national authorities to assess groups or passengers sitting next to a known suspect.

The collection of seating and baggage information in the API would allow many authorities to fill the gap in the current implementation of the PNR Directive, where many airlines (especially European operators) do not have the technical capability to send this information as part of the PNR message. The ability to use the information sent in a more complete PAXLST for law enforcement purposes would significantly increase the efficiency of the implementation of the PNR Directive.

3.4.3.3 MCA: assessment of coherence

The collection of API data for law enforcement purposes can ensure the coherence of EU legislation with the international framework (United Nations Security Council (UNSC) resolutions[90]) that calls for the use of API data in the fight against terrorism and organised crime.

The collection of API data for law enforcement purposes can also facilitate better harmonisation and standardisation between the application of the API and PNR Directives (overlaps and uncertainties were highlighted in the 2020 evaluation). Article 8 of the PNR Directive also refers to the collection of API data as part of the PNR data push and if these are collected in the normal course of business. The PNR Directive establishes an obligation for air carriers to transmit passenger data they hold in their reservation system, which is unverified information provided by passengers when

[90] United Nations Security Council Resolution 2396 (2017) states that: "'*Member States shall require airlines operating in their territories to provide API to the appropriate national authorities, in accordance with domestic law and international obligations, in order to detect the departure from their territories, or attempted travel to, entry into or transit through their territories, by means of civil aircraft, of foreign terrorist fighters".*

purchasing the ticket. The PNR Directive includes API data among the data to be sent by carriers in addition to reservation data only where air carriers have already collected such API data in the normal course of their business. The PNR Directive does not impose on carriers any obligation to collect additional data or to verify the accuracy of any of the data that are transferred.

There are several inconsistencies in the transposition and application of the two Directives at national level, with some Member States setting out the same sanction regime for API and PNR data (i.e. fines for the transfer of incorrect or incomplete PNR data) and/or using API data transferred within the framework of the PNR Directive for border control purposes rather than for the law enforcement purposes allowed by the PNR Directive.

Standardisation of the content of API message will support better information exchanges between the competent authorities of Member States. For instance, a closed and mandatory list of the type of information that all PIUs receive from air carriers will streamline data exchanges. Where risk profiles for suspects are not built on the same set of API data elements, this can become an obstacle for competent authorities in another Member State wanting to check data against their risk profiles (e.g. in instances of cooperation or investigation of transnational crimes).

To increase the added value of transmitted API data, this scenario also considers the use of the Universal Message Format (UMF) for API data in the context of law enforcement[91]. Such a format would be particularly relevant for API data collection on intra-EU flights and exchange of information between law enforcement databases. From a technological and operational perspective, the translation from API current formats (PAXLST) to UMF could be done by the carrier interface, with little impact on carriers' operations and processes (see policy option V). The conversion of API data to UMF is likely to make it easier to use by other/future applications (interoperable data), sparing national authorities' systems from dealing with the idiosyncrasies of legacy API data formats.

3.4.3.4 MCA: assessment of fundamental rights

As in scenario 1, the fundamental rights impacted by this scenario are (primarily) the right to privacy and the right to personal data protection. The impact of this scenario on these rights is similar to those identified in scenario 1, namely the data processing would entail an additional dataset compared to current baseline. The impacts on these rights are more significant than in scenario 1, as the data elements include seating and baggage information, which would give some information on a passenger's private life. No other data elements included in this scenario fall under sensitive categories of data.

This scenario essentially proposes requiring carriers to transmit a certain dataset to law enforcement authorities, which could already process such data where carriers collect them as part of the normal course of their business. The authorities receiving and processing this data would effectively be the PIUs. The 2020 evaluation and consultations for this Study confirmed that seating and baggage information are key to the prevention, investigation and prosecution of serious transnational crime, particularly organised crime and trafficking in human beings. Obliging the transmission of data elements contained in the MRZ of travel documents, as well as seat and baggage information, would yield more accurate results, reinforce identification of suspects, and increase the accuracy of matches and analysis performed by competent authorities, ultimately reducing false positives.

[91] UMF is a standard or agreement on the structure of the most important law enforcement concepts when they are exchanged across borders. In other words, UMF is a set of concepts (building blocks) to construct standard data exchanges for interconnecting dispersed law enforcement systems. It is not the internal structure of systems/databases (you are not required to change your national systems, legislation or processes) but rather an XML-based data format acting as a layer between them to be used whenever structured messages cross national borders. https://op.europa.eu/en/publication-detail/-/publication/3b2cc49f-72bb-419f-8742-eb21cd15e35c

While a future instrument on API will include a specific chapter on data protection to regulate the use and processing of passenger information collected, it is assumed that would be collected and processed for law enforcement purposes, the applicable data protection framework and safeguards should follow at a minimum the standards be that applicable to PNR data in the PNR Directive. Thus, the processing of API data for law enforcement purposes could be aligned to the data retention regime to that provided in the PNR Directive, namely five years (with data masked after six months). Any risk of unlawful access or use of the data would be mitigated by the existing technical and security features implemented by PIUs.

Table 11. Overview of the assessment for PO I Scenario 2

Policy option I, Scenario 2			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	N/A
		Enhance the security of citizens in the EU	■■■■□
	Specific objectives	Improve border checks	N/A
		Facilitate flow of legitimate travellers at the EU external borders	N/A
		Combat irregular migration	N/A
		Contribute to the fight against serious crime and terrorism	■■■■□
	Auxiliary objective	Public health control	N/A
Overall effectiveness assessment			🟦🟦🟦□□
Efficiency	***Costs***	Carriers	■■■■□
		Border management authorities	N/A
		Law enforcement authorities	■■□□□
	Benefits	Better passenger data	■■■■■
		Better risk analysis	■■■■□
		Better operational planning	■■■■□
		Better operational response	■■■■■
Overall efficiency assessment			🟦🟦🟦🟦□
Coherence	Streamline API with international standards		■■■■□
	Objectives of the Schengen Borders Code		N/A
	Objectives of EES Regulation		N/A
	Objectives of ETIAS Regulation		N/A
	Objectives of VIS Regulation (proposed recast)		N/A
	Objectives of the Interoperability Regulation		N/A
	PNR Directive objectives		■■■■■
Overall coherence assessment			🟦🟦🟦🟦🟦
Overall data protection and fundamental rights assessment			🟦🟦🟦🟦□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

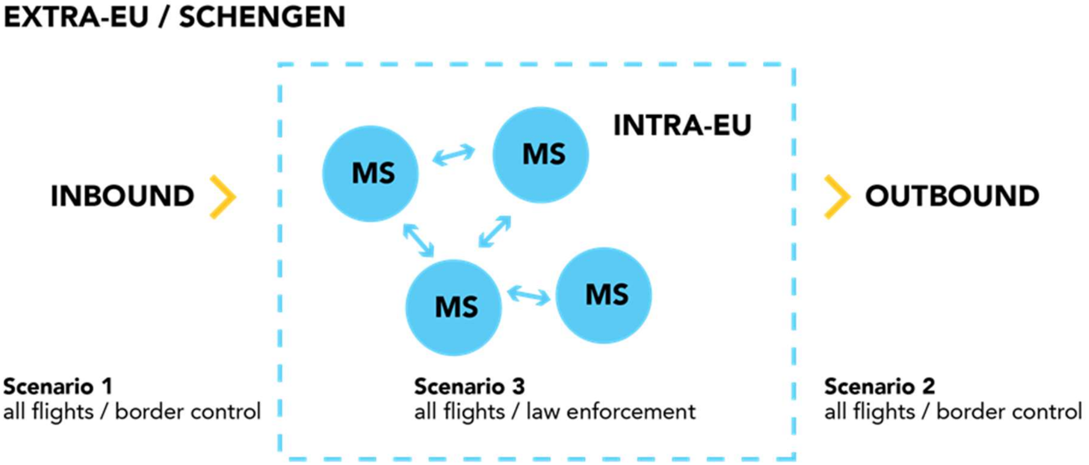
🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.5 Policy option II: Possible measures on the scope of the application of API-related obligations on air carriers' flights

Currently, the API Directive mandates the collection of API data for border control purposes on some extra EU/Schengen inbound flights. Member States' coverage of flights and routes subject to the obligations of collecting API data varies significantly. This policy option considers the extension of the scope of API to other flights and routes, covering only air transport. This policy option considers five scenarios, which differ in their focus on specific routes and in the purpose of the API data collection and processing (see Figure 6). Flights in the scope of each scenario include commercial flights, charter flights, cargo flights and business aviation.

Figure 6. Summary scenarios for policy option II


EXTRA-EU / SCHENGEN
INTRA-EU
INBOUND
OUTBOUND
MS
MS
MS
MS
Scenario 1
all flights / border control
Scenario 3
all flights / law enforcement
Scenario 2
all flights / border control

Source: ICF

3.5.1 Assessment of the baseline

Most Member States collect - or are planning to collect - API data on **all extra-EU inbound flights**[92], with several collecting data on selected flights[93] based on a risk analysis of routes for the purpose of migration management or law enforcement. The majority of Member States surveyed collect API data on all inbound flights for border management purposes.

Table 12. API data collected per type of flight (border management authorities)[94]

Risk based inbound extra-EU/Schengen	CH, DE, IT, PL	All inbound extra-EU/Schengen	AT*, BG, CZ, EE, ES, FI*, FR*, HU*, LU, LT*, SI*, SK*, RO
Risk based outbound extra-EU/Schengen	IT	All outbound extra-EU/Schengen	BG, CY, EE, FI*, FR*, HU, LT*, LU, SI*, SK*

Source: ICF elaboration from survey of border management authorities.

** Member States where, depending on the organisational set up and technical capabilities, API data are collected on both categories (risk-based flights and all flights).*

[92] 2020 evaluation: AT, BG, CZ, EE, ES, FI, HR, HU, IE, ISL, IT, LT, LV, MT, NL, PT, RO, SE, SI.
[93] 2020 evaluation: CH, DE, DK, FR, LU, NO, PL.
[94] 20 responses were received to the survey of border management authorities.

Implementing Member States request API data from selected flights based on risk analysis and/or policy priorities. Risk thresholds are a key factor for selecting flights for which to request API data and help to minimise the technical and human resources related to API collection[95]. However, the risk-based approach could result in security gaps as API data are not collected for certain routes considered lower risk by some Member States but higher risks by others.

Several Member States have extended the scope of API collection beyond that required by the Directive and also collect data for **outbound extra-EU/Schengen flights**[96]. This trend was confirmed by research carried out for this Study.

Under the PNR Directive, Member States can request data on all passengers on all inbound and outbound extra-EU flights[97].

The collection of API information on **intra-EU flights** is directly influenced by the scope of the PNR Directive[98]. Under Article 2(1) of the PNR Directive, Member States may decide to apply the Directive to intra-EU flights. As per the latest review of the application of the PNR Directive, a large majority of Member States have established PIUs with four Member States which did not fully transposed the Directive. All but one of the Member States have fully transposed the PNR Directive and have notified the Commission of their intention to apply it to intra-EU flights[99]. In the context of consultations carried out for this Study, Eight Member States consulted indicated that they request API data on intra-EU flights[100].

The "minimum harmonisation" approach adopted by the API Directive resulted in a variety of operational contexts, compounded by the implementation of the PNR Directive.

Discarded scenarios:

- ***Collecting API data systematically for all extra-EU inbound and outbound flights for law enforcement purposes***

As per the PNR Directive, PNR data are requested for all inbound and outbound flights. The PNR Directive mandates carriers to transmit API data to the PIU where these data are already collected. In combination with policy option I scenario 2, policy option II scenarios 1 and 2 propose requiring the collection of API data for border control purposes on all inbound and outbound flights. Following the logic of Article 8, para. 2 of the PNR Directive, this would allow PIUs to systematically collect API data for all inbound and outbound flights, as these elements will already be in the carriers' systems.

- ***Intra-Schengen flights for border management purposes***

A distinction should be made between intra-Schengen and intra-EU routes. The Schengen Borders Code does not provide the legal basis to collect passenger data on intra-Schengen routes, based on the free-movement principle applicable within the Schengen area. Collecting API data on intra-Schengen would equate to checking travel documents for border control purposes.

An exception can be made where temporary border controls are reinstated on internal borders. This has been used by certain Member States in the context of the fight against irregular migration to identify secondary movements and document fraud (checks on all passengers on

[95] Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, 2020.

[96] BE, BG, DK, EE, FI, FR, LT, PL, RO, SI, SK.

[97] Article 2(1) of the PNR Directive mentions the collection of PNR data for extra-EU flights, covering both inbound and outbound flights to/from outside the EU.

[98] 2020 evaluation.

[99] European Commission, Report on the review of Directive 2016/681, SWD(2020)128, Brussels, 24 July 2020, p.37.

[100] See Annex 7 for responses to the survey of border management and law enforcement authorities: AT, BG, DE (exceptional cases), FI, FR, HU, LT, SI (border management authorities); BE, DK, FR, HU, LV (law enforcement authorities).

all flights, while, in practice, data are only needed for selected routes/types of travellers/types of documents; however, not carrying out 'advanced' checks on passengers means less effective border controls).

The 2020 evaluation found that no Member State had used the API Directive as a basis to request API data on intra-Schengen flights, arguing that it could contravene the Schengen Borders Code provisions on introducing border checks at internal borders within the Schengen area. Most Member States that requested API data on intra-EU flights did so based on the PNR Directive and for law enforcement purposes, and only where air carriers collect the data in the normal course of their business. Therefore, the collection of API data on intra-Schengen flights for border control purposes was discarded in this Study.

From an operational perspective, intra-Schengen flights are shorter and require just-in-time collection and processing of data to potentially act on a passenger and carry out border checks. This is further substantiated by the short retention of data (24 hours) for border control purposes.

Implications of discarding this scenario: flights from an EU Member State to a Schengen Associated Country (CH, NO, IS) are not covered but are rarely considered high-risk routes.

- ***Domestic flights***

Several Member States appear to collect API data for domestic flights (BG, CY, DK, SI) – an option foreseen in neither the API Directive nor the PNR Directive. A scenario to collect API data systematically for domestic flights for law enforcement purposes was discarded. While security risks on domestic flights can be identified and API data are useful for identification, this type of requirement can be imposed on carriers under national law. Any action at EU level would require transnational or cross-border transport of passengers, in line with the subsidiarity principle outlined in the Treaty on European Union.

Table 13. Overview of assessment of baseline for policy option II

Policy option II, scenario 0			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	N/A
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at the EU external borders	■■■□□
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	N/A
	Auxiliary objective	Public health control	■■■□□
Overall effectiveness assessment			■■■□□
Efficiency	***Costs***	Carriers	■■□□□
		Border management authorities	■■■□□
		Law enforcement authorities	■■■□□
	Benefits	Better passenger data	■■□□□
		Better risk analysis	■■□□□
		Better operational planning	■■□□□
		Better operational response	■■□□□
Overall efficiency assessment			■■□□□
Coherence	Streamline API with international standards		■■□□□

	Objectives of the Schengen Borders Code	■■■□□
	Objectives of EES Regulation	■■■□□
	Objectives of ETIAS Regulation	■■■□□
	Objectives of VIS Regulation (and proposed recast)	N/A
	Objectives of the Interoperability Regulation	■■■□□
	PNR Directive objectives	N/A
Overall coherence assessment		■■■■□
Overall data protection and fundamental rights assessment		■■■□□

3.5.2 Policy option II, scenario 1: introduction of an obligation to collect API data systematically for all extra-Schengen inbound flights for border control and migration purposes

Summary of scenario 1

- This scenario proposes requiring the systematic collection of API data on all extra-Schengen inbound flights.
- This goes beyond the current situation whereby API data can be collected on a list of selected incoming flights, following a risk-based approach to data collection.
- This scenario thus mandates the transmission of API data for all incoming flights to the Schengen area, in line with the current geographical scope of the API Directive. The scope is extended to charter, cargo and business flights.
- The scenario enables the collection of data on all passengers and crew members, regardless of their nationality, crossing the external Schengen borders.

3.5.2.1 MCA: assessment of effectiveness

Collecting API data on all incoming flights to the EU could ensure systematic collection of API data from inbound flights and could result in enhanced external border checks. In any event, this collection will have to be performed in the future by carriers to comply with the obligations created by the ETIAS and EES Regulations.

The purpose of the data transmission - border control - will affect the geographical scope of the data transmission. Currently, the API Directive is mainly a Schengen acquis tool whereby EU Member States not applying the Schengen acquis had to notify their opt-in to request data. If future API legislation takes the form of a Regulation, these Member States will have to replicate similar obligations in national legislation or otherwise opt-in again.

3.5.2.2 MCA: assessment of efficiency

Costs

For air carriers, the widening of the scope of flights could increase their transmission costs. This assessment varies depending on the type of routes carriers operate.

The extension to other type of carriers would likely impact the infrastructure and maintenance costs of the transmission of API data (policy option I). While most large commercial airlines already have the capacity to collect such data via automated means, systems or applications, smaller airlines, including charters, collect such data manually (e.g. crew data collected in paper form). Carriers operating on routes not already subject to the obligation to collect API data would have to invest in additional system capabilities to comply with the new obligations. Additionally, the format and transmission time of the message containing crew information or baggage information from these carriers would have to cater for their specificities (i.e. receiving authority to accept .csv or .pdf formats). Indeed, the inclusion of crew would have an impact on carriers that do not traditionally fall within the scope of passenger data programmes, such as cargo operators. They have a more manual process to collect and transfer crew information, and a more systematic transfer request might imply more IT development or investment.

For border management authorities, an extension of scope could require modification of their API systems to receive and process additional data flows not previously collected. Similar to carriers, this would depend on the type of routes that national API systems already cover. The baseline scenario indicates that nearly half of Member States already collect API data on all inbound extra-Schengen routes. In Member States applying a risk-based approach and therefore requesting API data on a selected number of routes, this is justified by the technical capacity of the national API system (i.e. the threshold of passenger data it can process). For these Member States, an extension of the scope would imply additional costs.

The calculated costs across the relevant stakeholder groups are shown below. The full methodology used for the calculation of costs is provided in Annex 6.

Table 14. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs (rounded to the nearest million)** ***Scenario 1***
Air carriers	EUR 1,907.0 million
Border management authorities	EUR 11.0 million
Law enforcement authorities	Not applicable

Source: ICF estimates

Benefits

Consulted stakeholders (commercial carriers and national authorities) endorsed this extension of the scope of API data collection. It would allow border management authorities to maintain risk assessment and decisions internally. Transferring all API data on all passengers, regardless of their nationality or type of routes, would simplify the work streams for air carriers and other service operators involved in the transmission of data to competent authorities. Service operators flagged that while systems can be configured to send API data on a particular route (e.g. to a specific airport, Schengen or non-Schengen flights), this adds complexity to the processing of the data (e.g. exception rule handling) and ultimately leads to vulnerabilities as it increases the risk of missing data (for national authorities receiving data). Collecting only a sub-set of passenger data creates gaps and risks in the processing of data. Thus, this scenario would lead to better passenger data, increase legal certainty for carriers, and increase the operational capacity of competent authorities to process data.

3.5.2.3 MCA: assessment of coherence

This scenario would ensure consistency with the existing obligations stemming from the Schengen Borders Code, whereby all travellers crossing external borders are subject to a border check. Receiving API on all flights would enable authorities to effectively perform this duty (e.g. with advance notice of who is coming to the external border).

This is also in line with the provisions of Regulation 2017/458 requiring checks on travel documents data from third-country nationals and EU citizens alike[101].

Subject to implementation of the ETIAS (see policy option V), carriers would have to send API data for all flights to the CG, and an API batch for all passengers and crew to border authorities[102].

3.5.2.4 MCA: assessment of data protection and fundamental rights

From a data protection perspective, a risk-based approach is generally preferred as it impacts the rights to privacy and data protection of fewer passengers. The current baseline shows that this approach is not followed, however, nor would it lead to effective results in API processing.

This scenario would affect the rights of all passengers entering the EU's air borders (more than 260 million passengers per year[103]). As it would meet the general objective of ensuring effective checks at the external borders of the EU, processing data of all passengers is assessed as justified and proportionate to the objectives pursued.

Table 15. Overview of assessment for policy option II, scenario 1

Policy option II, scenario 1			Score
Effectiveness	*General objectives*	Improve the management and protection of EU external borders	■■■■■
		Enhance the security of citizens in the EU	N/A
	Specific objectives	Improve border checks	■■■■■
		Facilitate flow of legitimate travellers at the EU external borders	■■■■■
		Combat irregular migration	■■■■■
		Contribute to the fight against serious crime and terrorism	N/A
	Auxiliary objective	Public health control	■■■■□
Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	*Costs*	Carriers	🟧🟧🟧□□
		Border management authorities	🟧□□□□
		Law enforcement authorities	N/A
	Benefits	Better passenger data	■■■■■
		Better risk analysis	■■■■■
		Better operational planning	■■■■■
		Better operational response	■■■■■
Overall efficiency assessment			🟦🟦🟦🟦🟦
Coherence	Streamline API with international standards		■■■■■

[101] Regulation 2017/458 amending Regulation 2016/399 as regards the reinforcement of checks against relevant databases at external borders.

[102] In scenarios 0 (baseline) and scenario 1 of policy option V, carriers would still have to filter passenger data to submit data for visa-exempt and visa-holders to the carrier gateway and an API batch for all passengers and crew to border management authorities. In scenarios 2, 3 and 4, an iAPI message would be sent by a carrier to the carrier gateway that performs the interactive query/forwards the query/response to the Member State and returns the overall response to the carrier (depending on the scenario).

[103] Figures for 2019 (pre-Covid), Consultations for this Study with air industry associations.

	Objectives of the Schengen Borders Code	■■■■□
	Objectives of EES Regulation	■■■■□
	Objectives of ETIAS Regulation	■■■■□
	Objectives of VIS Regulation (and proposed recast)	■■■■□
	Objectives of the Interoperability Regulation	■■■■□
	PNR Directive objectives	N/A
Overall coherence assessment		🟦🟦🟦🟦🟦
Overall data protection and fundamental rights assessment		🟦🟦🟦🟦□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.5.3 Policy option II, scenario 2: Introduction of an obligation to collect API data systematically for all extra-Schengen outbound flights for border control and migration purposes

Summary of policy option II, scenario 2

- The API Directive neither mandates nor excludes the possibility to collect API data on outbound flights. This scenario proposes requiring the transmission of API data on all flights departing from the Schengen area.
- To support border controls, API data for outbound flights would be sent with a different timeframe than that for inbound flights to allow advance processing of the data prior to the exit border check at the airport. The transmission of API for outbound flights would then be extended to a first transmission at the end of check-in (40-60 minutes before departure) and a second transmission at flight departure to confirm that the passengers have left the territory.
- Like scenario 1, this scenario would enable the collection of data on all passengers and crew members crossing the external Schengen borders, regardless of their nationality.

3.5.3.1 MCA: assessment of effectiveness

For outbound flights, border controls are already performed by the authorities at exit border checks. However, the advance sharing of API data could help to speed-up these exit checks if the data are sent prior to flight departure. Several countries have imposed different timings for API data transmission, depending on whether the flight is inbound or outbound. For outbound flights, authorities could request a first transmission at the end of check-in, which could support the border checks performed on exit.

A second API message at flight closure would help to confirm that the passengers have actually left the territory and thus prevent overstayers. It would also complement the EES exit record, as API covers both third-country nationals and EU citizens.

It would also ensure consistency of checks to the Schengen area, both on entry and on exit. This would add value in supporting border guards' mission to prepare more thorough exit checks on certain types of cases (e.g. abducted children, victims and suspects in such crimes).

3.5.3.2 MCA: assessment of efficiency

Costs

A requirement to transmit API data on outbound flights would represent an increase in the volume of data and thus have a financial impact on carriers in respect of the cost of transmissions. The latter would need to re-programme their systems, and transmitting data to national authorities would need additional testing requirements. Many commercial airlines already collect API data on outbound flights – an outbound flight is also an inbound flight for third countries. These other countries are often collecting (or will be collecting) API data, thus the burden for acquiring the data is already present for carriers. While the requirements of third countries are similar to those of the EU (but not necessarily the same), the data protection and fundamental rights implications are equally present on such flights, whether EU Member State authorities receive this data or not.(they are the inbound API data for third countries), but the requirements of third countries are not always the same as the EU requirements. Further efforts at international level to align API requirements would help to reduce costs for carriers.

Likewise, border management authorities would incur additional costs to adapt their national API systems to additional volumes of data. This scenario could imply additional costs, especially if new IT solutions or applications were purchased, given the significant increase in data volume. If the outbound API data were to be used to support and prepare exit border checks, there would also be time-sensitivity in the process that might require authorities to invest in high-performing and rapid analysis tools.

Benefits

Air transport industry stakeholders argue that competition would suffer if such a requirement was imposed on air travel and not on other modes of transport.

From a border management perspective, the main benefits of collecting API data on outbound flights would be to support exit border checks or to fight organised crime at the border (e.g. human trafficking).

There could be some added value but the fact that exit checks take place already are performed on all passengers, including EU citizens, should also be considered. The outbound data would remain primarily a tool to better manage and prioritise cases at the border.

The calculated costs across the relevant stakeholder groups are shown below (see Annex 6 for detailed methodology and calculations).

Table 16. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs (rounded to the nearest million)** ***Scenario 2***
Air carriers	EUR 1,702 million
Border management authorities	EUR 22.5 million
Law enforcement authorities	Not applicable

Source: ICF estimates

3.5.3.3 MCA: assessment of coherence

This scenario would ensure consistency with international obligations on API data collection, which warrant the collection of API data on both inbound and outbound flights[104].

[104] See requirements on the use of passenger data stemming from the UN Security Council Resolutions 2178 (2014), 2396 (2017) and 2482 (2019).

With the scheduled entry in force of the EES in February 2022, the latter is expected to only record exits for third-country nationals from Schengen Associated Countries (ETIAS will only be deployed for inbound extra-Schengen routes). While a more comprehensive picture of outbound flows of travellers could help to reconcile differences among EU border management systems (e.g. EES, SIS), the added value of this scenario is limited as systematic checks on exit are carried out on both third-country nationals and EU citizens.

3.5.3.4 MCA: assessment of fundamental rights

The processing of API data on outbound flights for border management purposes is not yet a requirement under EU law, based on a risk-based approach or otherwise. Mandating the systematic transfer of API data on these routes might not meet the necessity test. Existing or future frameworks, such as Regulation (EU) 2017/458 on the reinforcement of checks against relevant databases at external borders (applicable both upon entry and exit) and the EES, would allow border management authorities to achieve the aim of checking travellers exiting the Schengen area. In addition, the imperative of receiving passenger data in advance of exit checks may not be viewed as necessary as entry checks, according to some stakeholders consulted.

Although some Member States request such data (based on national law), mandating the collection of API data in this scenario would impact the rights of a higher number of travellers (approximatively 260 million per year) than in policy option I, scenario 1. This option is thus likely to be disproportionate and to negatively impact the fundamental rights of passengers than measures assessed in scenario 1.

Table 17. Overview of the assessment for policy option II, scenario 2

Policy option II, scenario 2			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	N/A
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at the EU external borders	N/A
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	N/A
	Auxiliary objective	Public health control	N/A
Overall effectiveness assessment			■■■□□
Efficiency	***Costs***	Carriers	
		Border management authorities	
		Law enforcement authorities	N/A
	Benefits	Better passenger data	■■■□□
		Better risk analysis	■■■□□
		Better operational planning	■■■□□
		Better operational response	■■■□□
Overall efficiency assessment			■■■□□
Coherence	Streamline API with international standards		■■■■□

	Objectives of the Schengen Borders Code	■■■□□
	Objectives of EES Regulation	■■■■□
	Objectives of ETIAS Regulation	N/A
	Objectives of VIS Regulation (and proposed recast)	N/A
	Objectives of the Interoperability Regulation	N/A
	PNR Directive objectives	N/A
Overall coherence assessment		🟦🟦🟦□□
Overall data protection and fundamental rights assessment		🟦🟦□□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.5.4 Policy option II, scenario 3: Introduction of an obligation to systematically collect API data on intra-EU flights for law enforcement purposes

Summary of policy option II, scenario 3

- This scenario proposes requiring the collection of API data on intra-EU flights for law enforcement purposes.
- It would enable the collection of data on all passengers and crew members, regardless of their nationality.

3.5.4.1 MCA: assessment of effectiveness

Collecting API data on intra-EU flights would support law enforcement authorities in their risk analysis of travellers within the EU and complement PNR data already received for most intra-EU flights.

The scenario is effective if the scope of the API data collection is exhaustive, i.e. not following a risk-based approach. Combined with PNR data, this scenario would enhance the effectiveness of information analysis for law enforcement purposes. In more concrete terms, this would enable law enforcement authorities (PIUs) to receive verified API data (as part of PAXLST message/DCS system and not PNRGOV/reservation systems), allowing them to match watchlists more accurately.

This scenario would close an important gap and complement the PNR Directive, which allows (but does not oblige) Member States to collect PNR data on intra-EU flights. All but one of the Member States have notified the Commission that they collect PNR data on intra-EU flights. The collection of passenger data for intra-EU flights is an important 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 when they travel within the Schengen free-movement zone.

Collecting API data on intra-EU flights for law enforcement purposes could be done prior to the flight if it is legally required. The difficulty, however, would be to mandate carriers to perform a systematic ID check prior to boarding, as those checks would not be linked to border control. The API requirement for intra-Schengen flights could consider including only the requirement to collect passenger information, but not the obligation for the carrier to verify the information on the basis of an ID check. The resulting effect on data quality scenario could be mitigated by the approach considered in policy option IV mandating the automated collection of API data.

This scenario does not include the transmission of API data on a flight from a Schengen Associated Country to an EU Member State. Possible measures for Schengen Associated Countries would be to transcribe this type of requirement in national legislation or opt-in type provisions in EU legislation (on API and PNR).

3.5.4.2 MCA: assessment of efficiency

Costs

The volume of passengers on intra-EU flights is significantly more important than the volume of passengers whose API data are currently collected. A requirement to transmit API data on intra-EU flights would lead to an increase in transmission costs of the API data thus captured.

From an operational perspective, the collection of API data could also impact boarding and check-in time, thus affecting scheduling and the numbers of ground staff involved.

Carriers could have to invest in equipment for capturing a second MRZ from documents with an MRZ field other than ID cards or passports (e.g. visas and residence permits)[105]. To a certain extent, this will be part of the implementation of the future VIS Regulation (if the current proposal is adopted), as short-stay visas, long-stay visas and residence permits are covered in the Proposal amending the VIS Regulation (COM(2018) 302 final) in the context of the query mechanism.

Actors other than airlines would need to implement changes, as the EU has a number of small airports without the proper infrastructure to check travel documents.

The distinction between the obligation to collect the information and the obligation to verify the information might be an important factor in limiting the costs of this scenario: collection could be done automatically, while verification implies additional operational costs.

For national authorities, most PIUs already have the capacity to collect PNR data on intra-EU flights. Depending on the transmission protocols agreed with carriers, they also already receive API data (PAXLST message) on intra-EU flights.

The calculated costs across the relevant stakeholder groups are shown below (see Annex 6 for detailed methodology and calculations).

Table 18. Overview of costs across stakeholder groups

Stakeholder	**Estimated additional costs** ***Scenario 3***
Air carriers	EUR 2,250.0 million[106]
Border management authorities	Not applicable
Law enforcement authorities	EUR 23.0 million

Source: ICF estimates

Benefits

Most benefits would accrue for law enforcement authorities. Better passenger data and verified identification data/travel document data would support law enforcement

[105] This impact may however be lessened depending on the scenarios envisaged in policy option IV (see section 3.7), in particular if a solution whereby the passenger is equipped to read the MRZ.

[106] The costs are significant for air carriers owing to the fact that estimates have been calculated on the basis of the total population of air carriers in each Member States. However, not all air carriers may be affected, in which case the population of affected carriers will have to be revised downwards, which will likely lead to smaller overall costs under this Scenario. As regards the number of airlines that are currently collecting API data on this route specifically, the average is about 20 per cent of air carriers across the Member States (this is based on proxy data gathered on the proportion of passengers for whom API data are currently collected on this route as there are no other data).

authorities (PIUs) 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 ultimately reduce false positives in the processing of passenger data. Indeed, where a person is properly identified, it allows swifter analysis of information and strengthens the potential investigative elements.

The collection of API data on intra-EU flights could also help to decrease the number of temporary border controls on (air) borders, as the API data could be used to monitor movements in these exceptional cases instead of reinstating full physical border controls at airports. This scenario could therefore provide an alternative to the reintroduction of physical border controls at internal Schengen borders.

3.5.4.3 MCA: assessment of coherence

This scenario would promote EU Member States' compliance with commitments stemming from the UNSC resolutions on the threats posed by foreign terrorist fighters (Resolutions 2178 (2014), Resolutions 2396 (2017) and 2482 (2019)). Among other decisions, these Resolutions underline the need for Member States to request API data from airlines operating in their territories to detect the departure, attempted travel to, entry into, and transit through their territories. More specifically, this scenario would help national authorities to comply with this latter type of travel.

This scenario would ensure better coherence with the PNR Directive by overcoming discrepancies in the implementation of the API Directive (i.e. API data sent only if carriers have it in their systems). More accurate API data would support law enforcement authorities to track movements of suspicious individuals within the EU and to exchange information with other Member States[107].

3.5.4.4 MCA: assessment of data protection and fundamental rights

As in policy option II scenario 2, the API data in this scenario would be effectively processed by PIUs and thus be covered by the framework of the LED and further specified safeguards, such as the data protection and related safeguards in the PNR Directive.

The need to collect API data on all intra-EU flights can be demonstrated considering the limits of PNR processing under the PNR Directive[108]. The processing of API data in addition to the PNR data on intra-EU flights would increase the accuracy of matches in PNR systems (to the extent that API data are collected automatically from travel documents' MRZs by air carriers). Stakeholders confirmed that processing API data in conjunction with PNR data on intra-EU flights would be a valuable tool for criminal investigations.

The passenger flow on intra-EU flights is significantly higher than on inbound or outbound routes, representing some 489 million passengers prior to Covid-19[109]. The systematic collection of passenger data on these routes would interfere with the rights of EU citizens and third-country nationals travelling and residing in the EU. The right to free movement within the EU of EU citizens and third-country nationals legally residing in the EU should not be impacted. This scenario would not imply travel document checks similar to those at the external borders of the EU and data would be processed for law enforcement purposes only. In line with policy option II scenario 2, the objective would be to collect API data from travel documents, identity cards or residence permits that EU citizens and legally residing third-country nationals already hold. Additionally, the types of decisions inferred from the processing of API data on intra-EU routes would not

[107] See also SWD(2020) 128 final, p. 37.

[108] See European Commission, 2020, Staff working document accompanying the report on the review of the PNR Directive, SWD(2020) 128 final, p. 47-48, https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_swd-2020-128_en.pdf.

[109] Information based on passenger flows shared by air industry representatives (passenger flows in 2019). This includes any passenger flying within the EU, whether for transit or as last destination.

have consequences such as not letting a person board a plane or preventing travel to another Member State. From this perspective, the freedom of movement of EU citizens and legally residing third-country nationals would not be affected by this scenario.

The proportionality of processing API data on intra-EU flights could be further adjusted by adopting a risk-based approach (i.e. collecting and using data on selected, high-risk flights only).

Table 19. Overview of assessment for policy option II, scenario 3

Policy option II, scenario 3			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	■■■■□
	Specific objectives	Improve border checks	N/A
		Facilitate flow of legitimate travellers at the EU external borders	N/A
		Combat irregular migration	■■■■□
		Contribute to the fight against serious crime and terrorism	N/A
	Auxiliary objective	Public health control	N/A
Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	***Costs***	Carriers	🟧🟧🟧□□
		Border management authorities	N/A
		Law enforcement authorities	🟧□□□□
	Benefits	Better passenger data	■■■■■
		Better risk analysis	■■■■■
		Better operational planning	■■■□□
		Better operational response	■■■■■
Overall efficiency assessment			🟦🟦🟦□□
Coherence	Streamline API with international standards		■■■■■
	Objectives of the Schengen Borders Code		N/A
	Objectives of EES Regulation		N/A
	Objectives of ETIAS Regulation		N/A
	Objectives of VIS Regulation (and proposed recast)		N/A
	Objectives of the Interoperability Regulation		■■■■□
	PNR Directive objectives		■■■■■
Overall coherence assessment			🟦🟦🟦□□
Overall data protection and fundamental rights assessment			🟦🟦🟦□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.6 Policy option III: Possible measures on extending the scope of API instruments to other transport modes

Policy option III examines the potential extension of the obligation to collect API data to other modes of transport, namely rail carriers, maritime carriers and overland coach transport.

3.6.1 Rail carriers

Extending the obligation to collect passenger information to rail carriers

- Policy option III considers the possibility to impose an obligation on rail carriers to collect API data. Currently, there are no international standards for the collection of passenger data for rail operators. Article 26 of CISA provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. Rail carriers are excluded from this obligation. Consequently, rail operators – unlike air, sea and international bus and coach carriers – are not included in the EES/ETIAS Regulations and are exempt from the obligation to query the CG.

- In practice, two Member States collect API data for from rail carriers for outbound extra-EU journeys: Estonia and Finland[110]. In France, although national legislation specifies the collection of API data from train carriers, the obligation has yet to be implemented in practice[111].

- Several aspects are assessed under this policy option, including the type of route and the purpose for the extension:
  - Extending the API obligation to rail carriers for <u>extra-EU **inbound** routes for border management purposes</u> (scenario 1)
  - Extending the API obligation to rail carriers for <u>extra-EU **inbound** routes for law enforcement purposes</u> (scenario 2)
  - Extending the API obligation to rail carriers for <u>extra-EU **outbound** routes for border management purposes</u> (scenario 3)
  - Extending the API obligation to rail carriers for <u>extra-EU **outbound** routes for law enforcement purposes</u> (scenario 4)
  - Extending the API obligation to rail carriers for <u>**intra-Schengen** routes for border management purposes</u> (scenario 5)
  - Extending the API obligation to rail carriers for <u>**intra-EU routes** for law enforcement purposes</u> (scenario 6)
  - Extending the API obligation to rail carriers for <u>**domestic** routes for border management purposes</u> (scenario 7)
  - Extending the API obligation to rail carriers for <u>**domestic** routes for law enforcement purposes</u> (scenario 8).

- The technological, operational and organisational implications of these scenarios are assessed. Types of carriers and routes for the potential expansion of the collection of API data are examined, as well as whether specific types of carriers (e.g. international high-speed trains) could be obliged to collect and transmit passenger data.

[110] 2020 evaluation.

[111] Articles L232-1 and L232-4 of the Internal Security Code.

Discarded scenarios

- **Two international scenarios** were discarded – scenarios 5 and 6. The collection of passenger data for **intra-Schengen journeys for border control purposes** contravenes the absence of internal border controls (see Flixbus case[112]). The collection of passenger data for **intra-EU journey for law enforcement purposes** only makes sense if it complements the PNR data collected on the same journeys. To date, the PNR Directive does not mandate such collection of passenger data on intra-EU journeys and no Member State has implemented it (for other transport modes)[113].
- **Two domestic routes** scenarios were discarded – scenarios 7 and 8. In line with policy option II, this type of requirement can be imposed on carriers solely based on national law and thus cannot be mandated by a revised API legal instrument.

The analysis in the section below focuses on scenarios 1, 2, 3 and 4.

3.6.1.1 Assessment of baseline 0/baseline+[114]

Article 2(a) of the API Directive defines 'carrier' as any natural or legal person whose occupation it is to provide passenger transport by air only. Only two Member States collect API data from rail carriers[115]:

- In **Estonia**, rail companies must submit passenger data electronically to the border control unit. API data is collected from the Narva border crossing at the external border with the Russian Federation, a route operated by a single operator. Rail carriers to the Narva border crossing point must submit passenger lists. The State Borders Act was amended on 21 December 2014 to integrate the list of passenger data and the procedure for data transmission to the Regulation of the Minister of the Interior No. 42 of 28 August 2015 '*List of passenger data by air and rail, procedure and form for their transmission*'. The aim of the change was to organise the legal provision so that all carriers' (air, rail, sea) obligations are in the same legislation. This legal change enabled legal and natural persons providing international passenger transport on railways in Estonia to forward passenger lists electronically to the Police and Border Guard Board and to make it possible to carry out a preliminary check of lists. According to interviews carried out during the 2020 evaluation, the change made pre-control more effective.
- In **Finland**, Article 20a of the Act on the Processing of Personal Data by the Border Guard imposes an obligation on rail carriers to collect passenger data. Currently, the only train routes on which passenger data are collected are the Saint Petersburg-Helsinki and the Moscow-Helsinki routes.
- In **France**, national legislation specifies that API data are collected from air, sea and train carriers (Articles L232-1 and L232-4 of the Internal Security Code). While the obligation for train carriers exists in national legislation, it has not yet been implemented in practice. France participated in the discussions on API data from rail carriers with Belgium, the Netherlands and the UK for high-speed international trains, such as Eurostar.
- **Eurostar** is due to launch a PNR data-sharing pilot with Belgium. After scoping discussions with the UK and Belgian authorities, this is in development, but has been delayed by the COVID-19 pandemic and UK-EU Brexit negotiations. Mitie,

[112] CJEU, case C-412/17 - Touring Tours und Travel.

[113] Belgium launched a pilot project on PNR data collection for intra-EU journeys.

[114] Since Policy option III assesses the extension of scope to new modes of transport, no scoring table of the baseline is presented in this section as this is an entirely new scenario in itself.

[115] 2020 evaluation.

> Eurostar’s security provider in UK terminals, collects travel document (passport and national ID card) details of passengers exiting the UK at the UK-EU border after check-in and before boarding. The data are collected on behalf of UK Border Force based on the UK Immigration Act 1971, with Eurostar acting as a data processor on its behalf[116].

With regard to the baseline “+” situation, rail operators – unlike air, maritime and international bus and coach carriers – are not included in the EES/ETIAS Regulations and are exempt from the obligation to query the carrier gateway[117].

3.6.1.2 MCA: assessment of effectiveness

The assessment of effectiveness examines whether the four scenarios in policy option III could achieve the desired objectives, i.e. whether the potential expansion of the obligation to collect passenger data to rail carriers to extra-EU inbound and outbound rail travel could have positive effects for: improving border checks; facilitating flow of legitimate travellers; combating irregular migration; and contributing to the fight against serious crime and terrorism. It assesses whether specific types of carriers, such as international high-speed trains, could be obliged to collect and transmit passenger data.

The collection of API data aims to improve border control by collecting and transmitting passenger data in advance of arrival, facilitating border control by providing more time to check against EU, national and international databases and watchlists. The current obligations to collect passenger data from air carriers only does not provide for exact passenger itineraries, as passengers may undertake a combined transport trip and use other transport modes for onward travel. From border management and law enforcement perspectives, a passenger may conceal their movements by using a combination of transport modes (‘broken journeys’), preventing border management authorities from identifying their final destination.

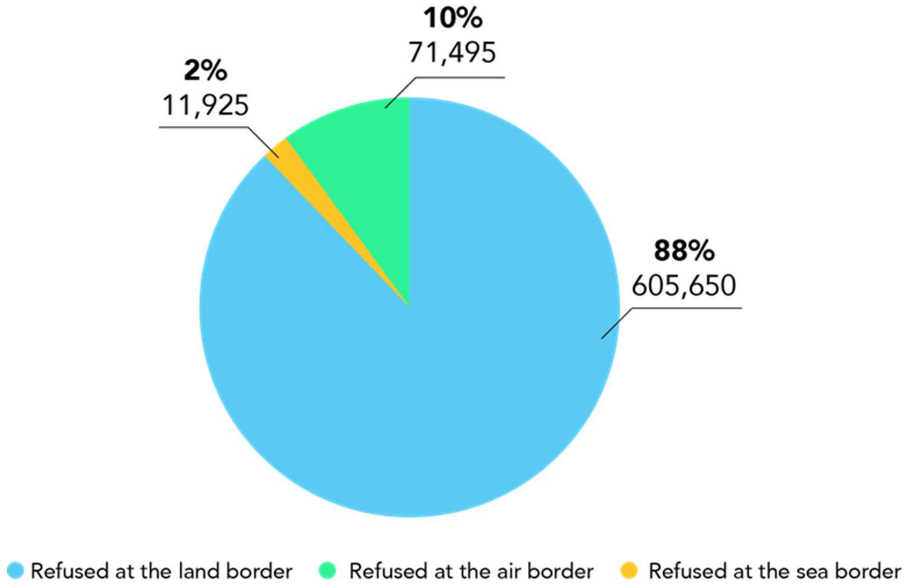
There are 14 Member States at the external borders of the EU: Bulgaria, Croatia, Estonia, Finland, Greece, Hungary, Ireland, Latvia, Latvia, Lithuania, Poland, Romania, Slovakia and Spain[118]. External traffic to and from the EU has shown a steady increase in recent years. Data (or proxy data) on the number of suspicious individuals or those attempting to enter the EU irregularly travelling by train on cross-border train journeys (scenarios 1-4) are not readily available. From a border management perspective (scenario 1), latest Eurostat statistics for 2019 show that 88% of entries refused are at land borders, compared to 10% at air borders and 2% at sea borders. Of the refusals at land borders, the highest number is Spain (483,455), followed by Poland (64,000), Hungary (13,500) and Croatia (12,355). Although these figures do not provide a complete picture (as they may include all forms of land border transport, including rail, bus, and non-passenger transport, such as road vehicles), they may indicate that land borders are more vulnerable to persons attempting illegal border crossings than either air and sea borders.

[116] Eurostar only sees this information at an anonymised aggregate level

[117] Article 26 of CISA provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. Rail carriers are excluded from this obligation.

[118] The countries neighbouring Schengen Associated Countries are not included in this number. The UK is an external border with France, Belgium, the Netherlands, Germany, Portugal, Spain, Denmark, Norway, Sweden, the Faroe Islands and Iceland.

Figure 7. Refusal of entry at external borders (2019)



Source: Eurostat [migr_eirfs].

In terms of the **volume of passengers**, the number of extra-EU international passengers is not readily available but ICF estimates from several sources (e.g. Eurostat, UIC and Rail Market Monitor Report) suggest up to 10 million international extra-EU rail passenger journeys in 2019, compared to 135 million international intra-EU rail passenger journeys.

Rail carriers are excluded from the obligation to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. They therefore only find out that a passenger has no valid visa only when crossing the border, which may lead to delays or other disruptions to the journey.

Stakeholders consulted pointed to a potential security gap if some modes of transport are not covered by the API obligations. Those obligations would only cover passenger transport modes and not passengers travelling by private road vehicles, meaning that a certain security gap could remain (suspicious individuals may opt to travel and cross the border by rental or private car, although there are other security tools and means of tracking, such as the European stolen vehicles database and licence plate recognition systems at external borders). Overall, the border management and law enforcement authorities surveyed see a need for the expansion of API data collection to rail carriers[119]. Two national law enforcement authorities observed that this need has been exacerbated by COVID-19, with air travel far more limited and perpetrators and victims now travelling more frequently on other means of transport, such as rail and coach.

[119] 62% of law enforcement authorities (8 responses) and 41% of border management authorities (7 responses) see the operational benefits of extending API obligations to international rail operators; 31% (4 responses) of law enforcement authorities and 41% (7 responses) of border management authorities are unsure/do not know, and 7% of law enforcement authorities (1 response) and 8% of border management authorities (3 responses) do not see any benefits. (Q16 in LEA survey and Q9 in BMA survey). Please see also Annex 7 and Annex 8.

Despite stakeholders noting the potential security gap, the feasibility of imposing obligations to rail carriers in practice has been called into question. Rail transport is a mass transport, open-access system, with a turn-up-and-go model of booking and traveling, and with a large volume of passengers (see Annex 8 for pre-COVID-19 data from 2019).

In addition to the density of the European rail network, industry stakeholders noted a number of physical infrastructure aspects of trains and train stations that complicate monitoring and enforcement of passengers alighting at their scheduled stop. There are multiple access points to the train – multiple doors on the train, multiple platforms, and sometimes multiple access points in large train stations. Another consideration is the infrastructure of train stations, where narrow platforms could present space constraints.

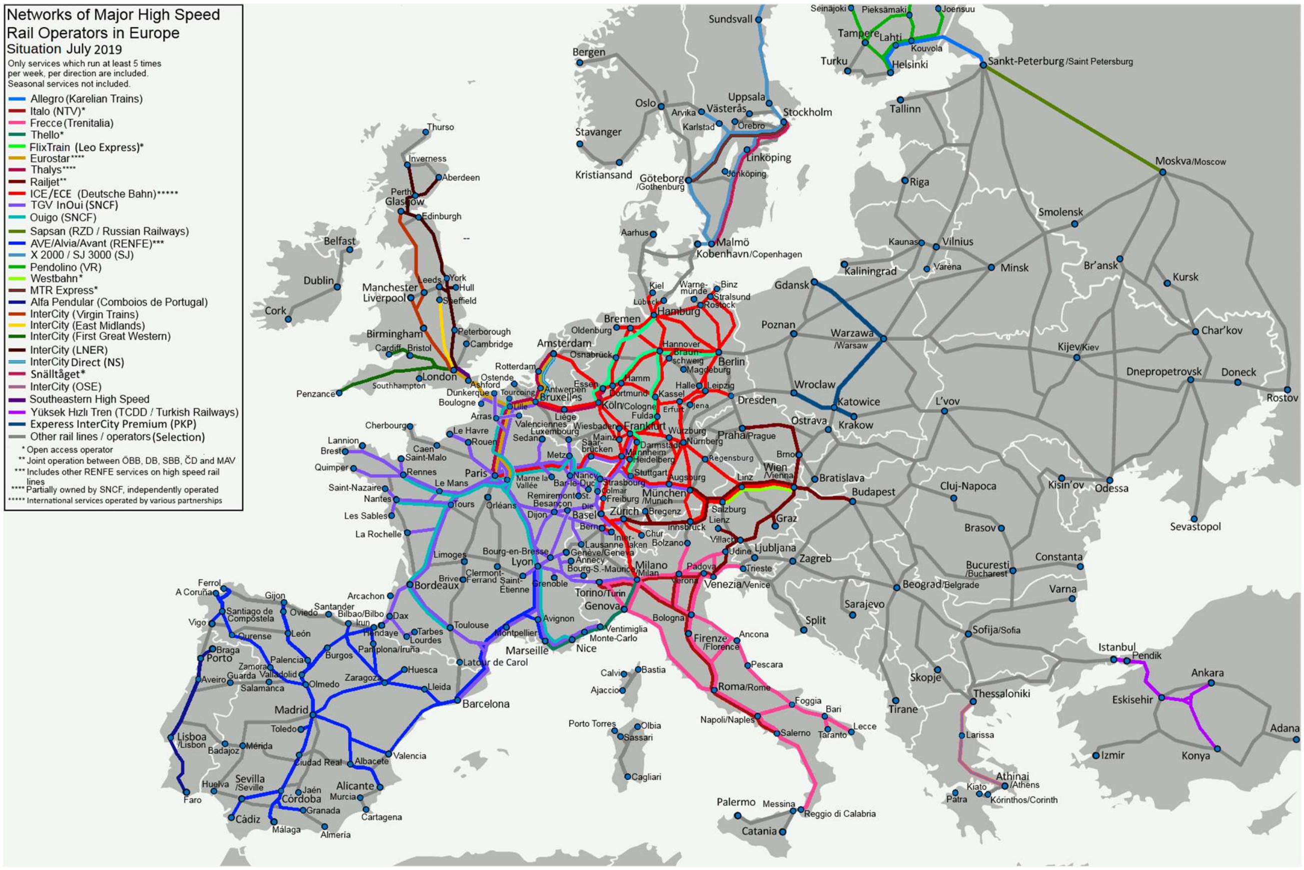
Given the feasibility issues in imposing API obligations on all rail carriers, the analysis focuses on whether such obligations can be imposed on specific train connections provided certain conditions are met. **A risk-based approach could be adopted whereby API data could be collected on certain international trains.** Provided that certain conditions are met would minimise the impact on the carriers' business model (unlike a blanket approach covering all rail operators):

- **Point-to-point journeys**: Connections with point-to-point journeys between large or medium cities with no intermediary stops or local traffic would ensure that passengers cannot alight from the train before or after their scheduled stop. Alternatively, some trains may be able to separate passengers in different coaches to facilitate identification of international passengers (e.g. where the doors do not open on local stops and passengers cannot alight before or after their scheduled stop).
- **Security screening and check-in infrastructure:** Provided that such infrastructure is already in place to allow for check-in or to capture passenger data prior to boarding (e.g. at large train stations, or verified onboard by train controllers prior to crossing the border), passengers can be screened on specific routes.

The stakeholders consulted suggested limiting the obligations to international high-speed connections, which meet such criteria in most cases. However, 'speed' may not be the defining factor, provided that other conditions are met. High-speed rail is defined as trains running with an average speed of 200 km/h and meeting certain conditions on the track, signalling systems and operations[120]. In practice, international extra-EU outbound and inbound high-speed train connections are very few - mainly to the UK (e.g. London to Brussels and Paris (Eurostar) and from Estonia and Finland to the Russian Federation (St Petersburg to Helsinki (Allegro) (Figure 8). The 2020 evaluation found that passengers on those connections already had their API data collected by carriers (see section 3.6.1.1).

[120] https://www.uic.org/com/enews/nr/596-high-speed/article/the-definition-of-high-speed-rail?page=thickbox_enews https://www.uic.org/com/enews/nr/596-high-speed/article/the-definition-of-high-speed-rail?page=thickbox_enews

Figure 8. Networks of major high-speed rail operators in Europe



Source:
https://ec.europa.eu/regional_policy/sources/docgener/work/2016_03_towards_urban_ind.pdf

In summary, the extension of API obligations to certain rail carriers for both border management and law enforcement purposes on a risk-based approach (provided some minimum conditions are met) could contribute to gaining a better situational picture of the movements of suspicious individuals. Considering the current COVID-19 situation, API data collection for both inbound and outbound journeys would also contribute to public health test-and-trace systems.

Table 20 (at the end of this section) presents the assessment of risk-based international trains of certain minimum conditions. In terms of inbound routes for both border management purposes (scenario 1) and law enforcement purposes (scenario 2), both are deemed beneficial for the achievement of the objectives. In terms of outbound routes for border management purposes (scenario 3) and law enforcement purposes (scenario 4), both scenarios are assessed as beneficial to achieving the objectives, as they would allow for better monitoring of cross-border movements. The added value of API data collection for law enforcement purposes (scenario 2 and scenario 4) would be more limited if there were no PNR data collection and processing on these routes, as API data would contain only the identity of the traveller and not additional reservation data. Including this possibility in a revised API instrument would yield effective results only in cases where the PNR Directive is also extended to rail transport (at least for international journeys).

3.6.1.3 MCA: assessment of efficiency

Rail transport has specific characteristics in terms of infrastructure, density of networks, passenger journey (check-in and boarding) and business models, which differ from the air and maritime sectors. Together, these elements complicate the monitoring and enforcement of passengers alighting at their scheduled stop. Imposing a blanket obligation on all rail carriers to collect API data would require substantial investment in physical infrastructure and changes to the business model of certain carriers, which may pose potential risks to the competitiveness of the sector.

The stakeholders - including border management authorities, law enforcement authorities, industry representatives and rail carriers - agreed that extending the scope of API would require significant investment to modify reservation systems, check-in and processes, and physical infrastructure (see Annex 7 for detailed survey responses). Hiring additional personnel might also be required in some cases. Industry representatives and carriers noted their concern that staff would need training to deal with entirely new processes requiring them to deal with highly confidential personal information.

Given the operational and technological challenges, the analysis focuses on international trains meeting certain conditions (see section 3.5.1.2).

Table 20. Overview of costs across stakeholder groups

Stakeholder	**Estimated additional costs** (rounded to the nearest million) ***Scenario 1***
Carriers	EUR 190.0 million
Border management authorities	EUR 80.0 million
Law enforcement authorities	EUR 80.0 million

Source: ICF estimates

3.6.1.4 MCA: assessment of coherence

There are currently no international standards on the collection of API data for rail carriers. At EU level, Article 26 of CISA provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. Rail carriers are excluded from this obligation. Consequently, rail operators – unlike air, sea and international bus and coach carriers – are not included in the EES/ETIAS Regulations and are exempt from the obligation to query the CG.

Like the API Directive, Article 1 of the PNR Directive specifies the scope as including ‘air carriers’, with data collection for other transport modes left to the discretion of the Member States (Recital 8 PNR Directive). In some Member States, PNR data are already collected from transport modes other than air traffic. The expansion of the scope of PNR to other transport modes is also under consideration. In November 2019, the Council Conclusions on widening the scope of the use of PNR data to forms of transport other than air traffic were adopted[121]. While some Member States welcomed the initiative and acknowledged the potential added value for preventing, detecting, investigating and prosecuting terrorist offences and serious crime, others voiced their concerns about the timing and (likely) legal, technical and financial challenges, notably with regard to fundamental rights and the principles of proportionality and necessity. The Council recommended that the European Commission conduct ‘*a thorough impact assessment*

[121] https://data.consilium.europa.eu/doc/document/ST-14061-2019-INIT/en/pdf

on widening the scope of the PNR Directive to cross-border forms of transport other than air traffic.'

Given the lack of international standards and EU legislation regulating the collection of passenger data for other carriers, no specific contradictions with current legal framework have been found. The potential extension of API data to rail carriers would neither contribute nor contravene any of the other legal documents as they currently stand. On the contrary, opening-up the possibility for Member States to collect data on specific rail journeys may future-proof the revised API instrument, given the expected revisions of the PNR Directive.

3.6.1.5 MCA: assessment of fundamental rights

The potential extension of scope of the API Directive to rail carriers would require processing a larger volume of personal data for passengers, albeit quite limited in volume in respect of international train connections.

The inclusion of other transport modes in the scope of a revised API instrument would contribute to gaining a better situational picture of passengers' final destinations and, to a certain extent, the potential detection of suspicious individuals or third-country nationals attempting to enter the EU irregularly.

Processing personal data for a large number of passengers for all extra-EU inbound and outbound rail journeys would not be justified. Furthermore, the specificities of rail travel (infrastructure, business model, etc) makes it unfeasible (at least in the short to medium-term) to impose such obligations on all passenger trains crossing the border. As a mitigating measure, the policy option suggests adopting a risk-based approach and focusing on specific trains, including high-speed international trains. This would limit the scope of API data collection and processing, as well as limiting the impact on the fundamental rights of passengers.

Table 21. Overview of assessment of effectiveness of policy option III, scenarios 1-4

Scenarios/ criteria			Scenario 1: Extra-EU inbound routes for border management purposes	Scenario 2: Extra-EU inbound routes for law enforcement purposes	Scenario 3: Extra-EU outbound routes for border management purposes	Scenario 4: Extra-EU outbound routes for law enforcement purposes
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□
		Enhance the security of citizens in the EU	N/A	🟦🟦🟦🟦□	N/A	N/A
	Specific objectives	Improve border checks	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Facilitate flow of legitimate travellers at the EU external borders	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Combat irregular migration	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Contribute to the fight against serious crime and terrorism	N/A	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□
	Auxiliary objective	Public health control	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
	Overall assessment effectiveness		🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□
Efficiency	**Costs**	Carriers	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
		Border management authorities	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
		Law enforcement authorities	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
	Benefits	Better passenger data	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
		Better risk analysis	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□

	Better operational planning	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Better operational response	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Overall assessment efficiency	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Coherence	Streamline with international standards	N/A	🟦🟦🟦□□	N/A	🟦🟦🟦□□
	Objectives of the Schengen Border Code	🟦🟦🟦□□	N/A	🟦🟦🟦□□	N/A
	Objectives of EES Regulation	🟦🟦🟦□□	N/A	🟦🟦🟦□□	N/A
	Objectives of ETIAS Regulation	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Objectives of VIS Regulation (and proposed recast)	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Objectives of the Interoperability Regulation	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	PNR Directive objectives	N/A	🟦🟦□□□	N/A	🟦🟦□□□
	Overall assessment coherence	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Data protection and fundamental rights		🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Overall assessment		🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.6.2 Maritime carriers

Extending the obligation to collect passenger information to maritime carriers

- This policy option considers the possibility to impose an obligation to collect API data on maritime carriers (i.e. maritime carriers). Article 26 of CISA provides that maritime carriers are obliged to assume responsibility for any travellers who are refused entry and to take all the necessary measures to ensure that travellers are in possession of the travel documents required for entry. The ETIAS/EES Regulations will also apply to maritime carriers.

- Several aspects are assessed, including the types of routes and the purpose for the extension as follows:
  - Extending the API obligation to maritime carriers for *extra-EU* ***inbound*** *routes* for border management purposes (scenario 1)
  - Extending the API obligation to maritime carriers for *extra-EU* ***inbound*** *routes* for law enforcement purposes (scenario 2)
  - Extending the API obligation to maritime carriers for *extra-EU* ***outbound*** *routes* for border management purposes (scenario 3)
  - Extending the API obligation to maritime carriers for *extra-EU* ***outbound*** *routes* for law enforcement purposes (scenario 4)
  - Extending the API obligation to maritime carriers for ***intra-Schengen*** *routes* for law border management purposes (scenario 5)
  - Extending the API obligation to maritime carriers for ***intra-EU*** *routes* for law enforcement purposes (scenario 6)
  - Extending the API obligation to maritime carriers for ***domestic*** *routes* for border management purposes (scenario 7)
  - Extending the API obligation to maritime carriers for ***domestic*** *routes* for law enforcement purposes (scenario 8)

- The technological, operational and organisational implications of these scenarios are assessed, including the types of carriers and routes for the potential expansion of the collection of API data.

Discarded scenarios

- Scenarios 7 and 8 were discarded. In line with policy option II, the **domestic collection** of API data can be imposed on carriers solely based on national law and thus cannot be mandated by a revised API legal instrument
- Scenarios 5 and 6 were discarded. The collection of passenger data for **intra-Schengen journeys for border management purposes** contravenes the principle of free movement of persons and the absence of border controls within the Schengen area. The collection of passenger data for **intra-EU journey for law enforcement purpose** does only make sense if it complements the PNR data collected on the same journeys. To date, the PNR Directive does not mandate such collection of passenger data on intra-EU journeys and no Member State has implemented it for other transport modes.
- The analysis thus focuses on scenarios 1, 2, 3 and 4.

3.6.2.1 Assessment of baseline 0/baseline+

There are several types of maritime carriers for different purposes, including passenger transport. According to the IMO, while there are no universally applicable definitions of ship types, specific descriptions and names are used within IMO treaties and conventions. A passenger ship is defined as a ship that carries more than 12 passengers[122].

Following the Schengen Borders Code and the Maritime Reporting Directive, all vessels coming to the Schengen area from a non-EU country must report passenger and crew data (as per FAL forms 5 and 6) to the maritime and border authorities. These forms are sent electronically 24 hours in advance via the NMSW. Maritime carriers are also subject to the obligation to check whether passengers are adequately documented before boarding. The IMO FAL Convention includes standards on the electronic transmission of data, which has been transposed in European law in the Maritime Reporting Formalities Directive and the Maritime Single Window Regulation[123]. These standards generally rely on EDIFACT and .xml.

The WCO has set up a Working Group for the development of a global standard for API and PNR data for cruise ships and a related compendium, as a precursor for other transport sectors[124]. The API and PNR global standard will be established for cruise ships and then expanded to ferries and (possibly) other maritime areas[125].

The 2020 evaluation found that 10 Member States already collect API data for maritime carriers[126].

With regard to the baseline+, maritime carriers will also need to check the ETIAS/EES gateway before boarding a passenger and they will have to query the CG for visa holders and visa-exempt travellers. The ETIAS Central Unit (managed by the European Border and Coast Guard Agency (Frontex)) will register the responsible party, which could be the ship owner or the company that sells the tickets (which could be an intermediary for cruise ships). Maritime carriers will thus query passenger information twice – once via the NMSW and once via the ETIAS/EES gateway.

3.6.2.2 MCA: assessment of effectiveness

The assessment of effectiveness examines whether the scenarios could achieve the desired objectives, i.e. whether the potential expansion of the obligation to collect API data to maritime carriers to extra-EU inbound and outbound travel (scenarios 1-4) would have positive effects for: improving border checks; facilitating flow of legitimate travellers; combating irregular migration; and contributing to the fight against serious crime and terrorism.

Similar to rail, the current obligation to collect API data from air carriers only does not provide for exact itineraries, as passengers may undertake a combined transport trip and use other transport modes for onward travel. From a border management and law enforcement perspective, passengers may conceal their movements by using a combination of transport modes (‘broken journeys’), preventing border management authorities from identifying their final destinations. Adding sea passenger transport to the scope of a revised API instrument would help to address this issue, albeit only partially if other transport modes are not also considered in scope.

The total number of maritime passengers embarking and disembarking in EU-27 ports was estimated at around 410 million in 2018, an increase of 5.6% on the previous year[127]. The number of inbound passengers to the EU-27 in 2019 was 208 million, while

[122] SOLAS - International Convention for the Safety of Life at Sea I/2.

[123] Article 5 of Directive 2010/65/EU and Regulation (EU) 2019/1239.

[124] See: http://www.wcoomd.org/en/media/newsroom/2020/october/14th-session-of-the-wco-iata-icao-api-pnr-contact-committee.aspx.

[125] Interview with an international organisation.

[126] AT, BE*, EE, ES, FI, FR, HU, IS*, MT, NO* (*planned API system).

[127] Eurostat (2018). mar_mp_aa and mar_mp_aa_cphd.

outbound passengers from the EU-27 accounted for 208 million[128]. The relatively small difference between the number of passengers disembarking (inward) and embarking (outward) in EU-27 could be explained by the fact that seaborne passenger transport in Europe is mainly operated by national or intra-EU-27 ferry services, with the same passengers counted twice in port statistics.

Refusals of entry at sea borders in 2019 (71,495) represented 10% of all refusals of entry at EU external borders.

Numbers of passengers may differ significantly between types of carrier. For example, cruise operators have a large number of travellers (guests), ranging from 700 to 6,000, reaching up to 9,000-10,000 when crew are included. An electronic system collecting passenger data should consider the specificities of transporting such a large number of travellers.

There are many different types of vessels and it is therefore essential to clarify the specific carriers that are within scope. There are differences in passenger data collection between ferries and cruise ships: while ferries collect passenger data before boarding the vessel, cruise ships appear to use a booking and a check-in system. Cruise ships generally have more developed systems, as they are subject to the IMO FAL Convention and to EU reporting obligations. A significant number of ferries operate primarily on intra-EU routes and are not subject to these reporting obligations.

The border management and law enforcement authorities from some Member States (e.g. Finland) observed during the interviews that they have noticed a significant increase in both maritime traffic and passengers in recent years. Those Member States in favour[129] of expanding the scope of API to maritime stated that a lot of maritime carriers are coming from countries considered at risk of migration flows or even terrorism. The expansion of scope could contribute to mitigating border risks and facilitate faster border checks. The law enforcement authorities consulted expressed the view that the standardisation of API data collection across these other transport modes would be highly beneficial. The current situation is critical, as every non-air carrier collects and stores passenger information in its own way.

Currently, passenger manifests are sent via the maritime single window. With the adoption of the ETIAS/EES Regulations, the maritime sector will need to consult first the EES/ETIAS databases before the departure of ships and then will need to be subject to two requirements on the transfer of passenger information to the border authorities: one stemming from the EMSW National sand one based on ETIAS requirements. In view of the adoption of the EMSW, industry stakeholders expressed the need to minimise new obligations on carriers and a preference for the data to be collected only once, through the EMSW. While, in principle, the industry does not have specific concerns about online booking and check-in in advance, concerns were raised about the infrastructure at ports (e.g. people in cars boarding ferries) and the verification requirements of the travel document before boarding, as ports and ships do not always have a check-in system (unlike airports). At present, only quick, visual checks of passenger passports/IDs are performed before boarding (mainly on travel operated by ferries). Due to large volumes of passengers, the processing of personal information before boarding could have significant implications for the length of stay at the port before embarkation. There is also an environmental component: every minute added to a vessel's port stay means that the ships' travel time has to be quicker, leading to exponentially increasing emission of greenhouse gases.

[128] Eurostat (2019). mar_mp_aa. No origin countries were specified and no separation between intra-EU/extra-EU data.

[129] 62% of law enforcement authorities (8 responses) and 29% of border management authorities surveyed (6 responses) see operational benefits of extending the obligations to international rail operators; 31% (4 responses) of law enforcement authorities and 42% (4 responses) of border management authorities are unsure/do not know; 7% of law enforcement authorities (1 response) and 29% of border management authorities (4 responses) do not see any benefit.

Overall, there is a consensus that extending API obligations to maritime carriers would contribute to better monitoring of movements on entry and exit, as well as the technical capabilities in terms of reservation and booking systems are more advanced than other modes of transport. In contrast to land transportation, where the practical feasibility of extension of scope to all such carriers is in doubt, put into question, in the case of maritime, the main concerns for the maritime sector relate to are around the verification of the travel document, the timing of transmission of passenger data, and as well as the harmonisation of data requirements via different systems (- i.e. reusing the information already collected via the Maritime Single Windows in line with the Reporting Formalities Directive, which already applies to all vessels (apart from those ones exempted in Article 15 of EU Directive 2002/59)) to be used by Member States authorities as API data. The issue of leisure boats was not considered. Despite its similarity to business aviation travel, this category does not include a large volume of passengers although it has similar risk profiles.

For scheduled passenger services such as ferries or local cruises, the data elements contained in FAL forms 5 and 6 are sufficient to perform a watch list check of travellers, together with basic targeting. For ferries, the vehicle number should also be considered for checks against the stolen vehicle databases (SIS, Interpol). For unscheduled services or irregular operators, additional information could be requested for risk assessment purposes, such as the ship ownership, the last ports of call. Collection of FAL form 1, as well as of some of the information provided under the security obligations of the SOLAS Convention, could give the competent authorities additional information on the purpose of the trip and profile of the ship operations.

The challenge with some routes is that they are short (e.g. between Morocco and Spain) and border management authorities do not have time to process the data, or the passenger manifest arrives too late for any meaningful border control action. These difficulties are linked to the quality of the data provided, which requires significant manual processing, and to the lack of established processes at the port of origin. A harmonised standard for the transfer of API data with an agreed format and transfer protocol should help with these difficulties. The use of mobile apps for the automated collection of the MRZ should also help.

3.6.2.3 MCA: assessment of efficiency

The border management and law enforcement authorities surveyed indicated that the potential extension of the scope of API would require changes in operational guidelines, modification of IT systems, training of personnel, and (to a lesser extent) organisational restructuring and hiring of additional personnel. In their responses to the industry survey, three maritime carriers estimated that they would require substantial modifications and investment in reservation and check-in systems, physical infrastructure and in hiring additional staff.

Table 22. Overview of costs across stakeholder groups

Stakeholder	**Estimated additional costs** (rounded to the nearest million) ***Scenario 1***
Carriers	EUR 1,300.0 million
Border management authorities	EUR 80.0 million
Law enforcement authorities	EUR 80.0 million

Source: ICF estimates

3.6.2.4 MCA: assessment of coherence

At EU level, Article 26 of CISA provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. The future implementation of the ETIAS and EES Regulations will apply to maritime carriers.

Directive (EU) 2017/2109 on the registration of persons on passenger ships mandates the collection, recording and transmission (via the National Maritime Single Window) of onboard passengers' data (names, nationality, gender, data of birth).

Similar to the API Directive, Article 1 of the PNR Directive mandates the collection of passenger data by air carriers. However, the API Directive leaves it to Member States to decide whether to retain or introduce additional obligations for some categories of other carriers.

3.6.2.5 MCA: assessment of fundamental rights

Extending the scope of a future API instrument to maritime carriers would not create additional processing of data by national authorities, as maritime carriers already transmit passenger and crew data to border management authorities.

Law enforcement access and use of passenger data collected at maritime borders should be clearly regulated either in national legislation and/or in a revised PNR Directive.

3.6.3 Overland coach carriers (buses and coaches)

Extending the obligation to collect passenger information to overland coach carriers

The assessment considered the possibility of imposing an obligation to collect API data on overland coach carriers. As per Article 26 of CISA, on extra-EU inbound routes, international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. The future implementation of the ETIAS and EES Regulations will apply to overland coach transport operators.

Several aspects are assessed, including the types of routes and the purpose for the extension:

- Extending the API obligation to land carriers for ***extra-EU inbound** routes* for border management purposes (scenario 1)
- Extending the API obligation to land carriers for ***extra-EU inbound** routes* for law enforcement purposes (scenario 2)
- Extending the API obligation to land carriers for ***extra-EU outbound** routes* for border management purposes (scenario 3)
- Extending the API obligation to land carriers for ***extra-EU outbound** routes* for law enforcement purposes (scenario 4)
- Extending the API obligation to land carriers for ***intra-Schengen routes*** for law border management purposes (scenario 5)
- Extending the API obligation to land carriers for ***intra-EU routes*** for law enforcement purposes (scenario 6)
- Extending the API obligation to land carriers for ***domestic routes*** for border management purposes (scenario 7)
- Extending the API obligation to land carriers for ***domestic routes*** for law enforcement purposes (scenario 8)

The technological, operational and organisational implications of these scenarios are assessed, including the types of carriers and routes for the potential expansion of the collection of API data.

Discarded scenarios

- Scenarios 7 and 8 were discarded. In line with policy option II, the **domestic collection** of API data was discarded as this type of requirement can be imposed on carriers solely based on national law and thus cannot be mandated by a revised API legal instrument.
- Scenarios 5 and 6 were discarded. The collection of passenger data for **intra-Schengen journeys for migration management purposes** contravenes the absence of internal border controls (see Flixbus case[130]). The collection of passenger data for **intra-EU journeys for law enforcement purposes** only makes sense if it

[130] CJEU, case C-412/17 - Touring Tours und Travel: In 2018, the Court of Justice of the European Union (CJEU) ruled against a national measure requiring private coach transporters crossing internal borders to check the documents of the passengers on board and refuse access to those not providing a passport or residence permit. The case concerns two coach companies travelling to Germany from the Netherlands and Belgium. Since 2013, German authorities recorded a significant number of third-country nationals who travelled without the necessary travel documents. After an initial warning, the Directorate of the Federal Police issued the companies with a prohibition order, together with a fine for each new infringement, requiring the transport service providers to check the passengers before boarding and to refuse access to those who were not in possession of the required documents. The Court ruled that this is prohibited under Article 21(a) of Regulation No 562/2006 (Schengen Borders Code) as it has an effect equivalent to that of border checks.

complements the PNR data collected on the same journeys. To date, the PNR Directive does not mandate such collection of passenger data on intra-EU journeys and no Member State has implemented it.

The analysis thus focuses on scenarios 1, 2, 3 and 4.

3.6.3.1 Assessment of baseline 0/baseline+

Article 2(a) of the API Directive defines 'carrier' as any natural or legal person whose occupation it is to provide passenger transport by air only.

Several Member States have national legislation with the legal basis to collect passenger data from overland coach carriers. Unlike rail or maritime carriers, however, no Member State has proceeded to the practical implementation of such an obligation (even in pilot form). None of the national authorities surveyed reported the collection of API for bus/coach travel in their Member States.

The future implementation of the ETIAS and EES Regulations will apply to overland coach transport operators (as of 2025).

3.6.3.2 MCA: assessment of effectiveness

The assessment of effectiveness examines whether the scenarios could achieve the desired objectives, i.e. whether the potential expansion of the obligation to collect passenger data to land carriers for extra-EU inbound and outbound travel would have positive effects on: improving border checks; facilitating flow of legitimate travellers; combating irregular migration; and contributing to the fight against serious crime and terrorism.

Data on extra-EU coach traffic is limited and not readily available, with Member States reporting on an anecdotal basis. The data indicate considerable annual growth in international passengers in a number of Member States, such as Czechia, Estonia and Poland (see Table 23 for numbers of international passengers in 2018 in seven Member States). The latest Eurostat statistics for 2019 show that 88% of refusals of entry were at land borders, compared to 10% at air borders and 2% at sea borders (see section 3.6.1).

Table 23. International coach passengers (thousands) (2009-2014)

Member State	2009	2010	2011	2012	2013	2014
Croatia		2,466	2,100	2,347	2,205	1,612
Czech Republic	1,212	1,130	1,598	1,980	1,981	2,088
Estonia	399	488	555	633	734	809
Italy				837		
Lithuania	300	300	300	300	300	400
Poland					2,789	3,255
Portugal			331	288	372	356
Slovenia				268	310	260
Slovak Republic					1,543	
Sweden	806	754	662		512	

Source: European Commission, Study on Passenger transport by coach in Europe (2016)

Table 24. Number of international passengers, 2018

Member State	Number of passengers
Bulgaria	1,825,100
Estonia	1,895,000
Croatia	1,281,000
Hungary	4,431,800
Poland	5,200,000
Portugal	1,214,490
Romania	2,448,000

Source: European Commission, Study on Passenger transport by coach in Europe (2016)

Currently, there are no international standards for the collection of passenger data by coach operators. Commission Regulation (EU) 361/2014[131] provides for the standardisation of documentation for international carriage, including international occasional bus services and cabotage of passengers by coach and bus. The Regulation provides for 'journey forms' in paper version ('*books of 25 forms, in duplicate, and detachable*') but also provides that '*Member States shall take all necessary measures to adapt these requirements to computerised processing of journey forms'.* Annex I to the Regulation provides the journey form template, which only includes 'total number of passengers' and does not include personal data of individual passengers[132]. Unfortunately, no coach operators participated in this Study (a number of refusals were received from coach operators) and the practice has not been confirmed with coach operators. Interviews with industry representatives (International Road Transport Union (IRU)) confirmed that journey forms are routinely collected, and some operators may collect very limited personal data of passengers for safety and security reasons.

Industry representatives pointed to a number of sector-specific limitations in relation to physical and digital infrastructure. The digitalisation of the road transport sector has remained somewhat limited and collection of passenger data is not a specific focus for coach operators. With regard to physical infrastructure, not all bus terminals have multiple lanes. Concerns were also expressed at the expectation that bus drivers would check travel documents, which is outside of their current remit and training.

The coach transport sector in Europe is decentralised, with many small and medium-sized companies[133] having small fleets of 3-100 coaches. Data on the number of extra-EU cross-border journeys by coach are not readily available. COVID-19 saw a significant decrease in the number of connections, making it difficult to extrapolate connection information from current timetables.

Similar to other transport modes, the current obligation to collect passenger data from air carriers only does not provide for exact itineraries, as passengers may undertake a combined transport trip and use other transport modes for onward travel. From a border management and law enforcement perspective, passengers may conceal their movements by using a combination of transport modes ('broken journeys'), preventing border management authorities from identifying their final destinations.

The stakeholders consulted confirmed the potential for a security gap if some modes of transport are not covered by the API obligations. The obligations miss passengers travelling by private road vehicles (suspicious individuals may opt to travel and cross

[131] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0361&from=EN

[132] Euro Controle and the IRU have published a guide on how to complete the journey form: https://www.euro-controle-route.eu/sites/ECR/uploads/files/en-0324-eu-journey-form-web.pdf

[133] Industry estimates of 3,000-5,000 coach companies in the EU.

the border by rental or private cars, although there are other security tools and means of tracking, such as the European stolen vehicles database and licence plate recognition systems at external borders). Overall, the border management and law enforcement authorities surveyed see the need for the expansion of API data to overland coach carriers[134]. Some border management authorities noted that this would improve risk-based profiling of international passengers and increase the rate of detection of persons identified as irregular migrants.

Similar to rail carriers, a risk-based approach could be adopted whereby API data could be collected on cross-border buses and coaches provided certain conditions are met - this would minimise the impact on the carriers' business model (as opposed to a blanket approach covering all operators):

- **Security screening and check-in infrastructure:** Provided that such infrastructure is already in place to allow for check-in (e.g. at bus terminals) or checks before boarding, passengers can be screened on specific routes.
- **Reconciliation and control of the list of onboard passengers**: The bus operator would implement strict access control to the bus and perform a reconciliation and control after each stop and update the passenger list accordingly.
- **Automation of data transfers:** The bus operator would automate the transfer of the passenger data after each stop or update of the list of passengers on board.

In summary, the extension of API obligations to extra-Schengen international bus carriers, for both border control and law enforcement purposes and for both inbound and outbound purposes, with a risk-based approach and provided some minimum conditions are met (i.e. point-to-point journeys and security screening and check-in infrastructure), would contribute to a better situational picture of the movements of suspicious individuals. In light of COVID-19, API data collection for inbound and outbound journeys would also contribute to public health test-and-trace systems.

3.6.3.3 MCA: assessment of efficiency

According to the industry representatives consulted, the collection of API through reservation systems of coach and bus carriers is very limited. Imposing an obligation on carriers to collect and transmit passenger data would require investment in IT systems. The fragmentation of the sector is such that this would mean a lot of small and medium-sized companies having to invest in IT systems. Possible solutions to lessen the financial cost include a mobile app and a Near Field Communication (NFC) reader (see policy option IV for more detail).

The border management and law enforcement authorities consulted saw the benefits of expanding the API scope to coach operators as better security screening and improving risk-based profiling of international passengers. No specific benefits were identified from the operators' perspective. In the event of scope expansion, the authorities would envisage a need for changes in operational guidelines, modification of API systems to receive and process such datasets, training of personnel, and (to a lesser extent) hiring of additional personnel (see Annexes 6, 7 and 8 for details).

In view of COVID-19, coach and bus carriers declined to participate in the study and no anecdotal information was found on the specific practices and processes for collecting passenger data.

[134] 62% of law enforcement authorities (8 responses) and 50% of border management authorities surveyed (8 responses) see operational benefits of extending the obligations to international coach operators; 31% (4 responses) of law enforcement authorities and 39% (7 responses) of border management authorities are unsure/do not know; 7% of law enforcement authorities (1 response) and 11% of border management authorities (2 responses) do not see any benefits.

Table 25. Overview of costs across stakeholder groups

Stakeholder	Estimated additional costs (rounded to the nearest million) *Scenario 1*
Carriers	EUR 138.0 million
Border management authorities	EUR 80.0 million
Law enforcement authorities	EUR 80.0 million

Source: ICF estimates

3.6.3.4 MCA: assessment of coherence

There are no international standards on the collection of API data for overland coach and bus carriers. At EU level, Article 26 of CISA provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who are refused entry and to take all necessary measures to ensure that travellers are in possession of the travel documents required for entry. The future implementation of the ETIAS and EES Regulations will apply to overland coach transport operators.

Similar to the API Directive, Article 1 of the PNR Directive mandates the collection of passenger data by air carriers. However, the API Directive leaves it to Member States to decide whether to retain or introduce additional obligations for some categories of other carriers.

3.6.3.5 MCA: assessment of fundamental rights

The inclusion of overland coach carriers (buses and coaches) in the scope of a future API instrument would contribute to a better situational picture of the final destination of the passenger and, to a certain extent, to the potential detection of suspicious individuals and third-country nationals attempting to enter the EU irregularly. However, it would require processing additional volumes of personal data for passengers, on both inbound and outbound routes increases, significantly increasing the impact on data protection and privacy. Given the business model operated by carriers in this mode of transport (variable size of companies and numbers of passengers transported), a number of risks could emerge in the processing of passenger data. Mitigation measures, such as the roll-out of mobile app solutions for the collection and transfer of passenger data to competent authorities could reduce such risks.

Table 26. Overview of assessment of effectiveness of policy option III, scenarios 1-4

Scenarios/ criteria			**Scenario 1: Extra-EU inbound routes for border management purposes**	**Scenario 2: Extra-EU inbound routes for law enforcement purposes**	**Scenario 3: Extra-EU outbound routes for border management purposes**	**Scenario 4: Extra-EU outbound routes for law enforcement purposes**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□
		Enhance the security of citizens in the EU	N/A	🟦🟦🟦🟦□	N/A	N/A
	Specific objectives	Improve border checks	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Facilitate flow of legitimate travellers at the EU external borders	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Combat irregular migration	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
		Contribute to the fight against serious crime and terrorism	N/A	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□
	Auxiliary objective	Public health control	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
	Overall assessment effectiveness		🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□	🟦🟦🟦🟦□
Efficiency	**Costs**	Carriers	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
		Border management authorities	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
		Law enforcement authorities	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□	🟧🟧🟧□□
	Benefits	Better passenger data	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
		Better risk analysis	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□

	Better operational planning	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Better operational response	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Overall assessment efficiency	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Coherence	Streamline with international standards	N/A	N/A	N/A	N/A
	Objectives of the Schengen Border Code	🟦🟦🟦🟦🟦	N/A	🟦🟦🟦🟦🟦	N/A
	Objectives of EES Regulation	🟦🟦🟦🟦□	N/A	🟦🟦🟦🟦□	N/A
	Objectives of ETIAS Regulation	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Objectives of VIS Regulation (and proposed recast)	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	Objectives of the Interoperability Regulation	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
	PNR Directive objectives	N/A	🟦🟦🟦□□	N/A	🟦🟦□□□
	Overall assessment coherence	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Data protection and fundamental rights		🟦🟦🟦🟦□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□
Overall assessment		🟦🟦🟦🟦□	🟦🟦🟦□□	🟦🟦🟦□□	🟦🟦🟦□□

Legend

⬛ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.7 Policy option IV: Possible measures on improving API data quality

This option examines the possible scenarios for improving the quality of API data. Since the 2012 evaluation, the insufficient degree of harmonisation of quality and related sanctions have been considered an impediment to the effective implementation of the API Directive.

3.7.1 Assessment of the baseline

Effectiveness

The 2020 evaluation found that not all Member States' authorities perform systematic data quality checks prior to processing the data to determine whether human intervention is required[135]. Data quality verification processes vary substantially between Member States. While some of the Member States reported carrying out verification during the physical checks of passengers by the border control unit[136], others have developed complex procedures involving several levels of quality assurance[137].

The industry surveys (see Annexes 7 and 8) show that half of the responding air carriers (10 of 20) have processes and/or technologies in place to enhance data quality before it is transmitted. These measures range from a mandatory 'swipe' through an MRZ reader, to automatic semantic or syntax checks of the self-declared data entered to identify incorrect or incomplete data entered[138].

The 2020 evaluation also found that Member States receive passenger data at multiple points in time, with some receiving the same data multiple times[139]. The timing of API data transfer has an impact on the completeness - and therefore the quality - of the data transferred.

The 2020 evaluation also showed that while most Member States[140] control the quality of data received provided by engaging with the carriers, some[141] relied on sanctions. While Article 4 of the Directive sets minimum and maximum sanction amounts, it allows significant leeway in transposition. Without a defined data quality threshold to trigger sanctions, Member States have divergent rules, do not impose sanctions at all, or prefer negotiations.

Fourteen Member States imposed fines for the violation of obligations related to the transmission of API data[142]. The 2020 evaluation also found that different amounts were applied to carriers failing to collect and correctly transmit API data (ranging from EUR 100 in Germany to EUR 500,000 in Ireland).

The 2020 evaluation did not draw firm conclusions on the impact of sanctions on data quality, as few Member States were able to provide reliable data. Differing approaches to enforcement, on the other hand, were perceived to hinder compliance efforts, increase the risk of non-adherence, and reduce potential corrective actions imposed by national authorities.

The effectiveness of the status quo was assessed as 3/5 overall, largely because data quality is central to an effective API system and achievement of its objectives. While there remain some issues with data quality, they are not at a level that fundamentally undermines the objectives of the Directive, although there is scope for improvement.

[135] DE, ES, FI, FR, HR, IE, LT, NO, PL, SE, SI, SK.

[136] AT, DE, HR, IE, NO, SK.

[137] BG, CH, SI, SK.

[138] CRM Feasibility Study Report; interviews with industry;

[139] DK, EE, ES, IE, LT, PL, PT, SK.

[140] BE, BG, DK, EE, EL, FR, IE, LU, NL, PT, SE, SI, SK, UK, CY, NO, ISL

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

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

Efficiency

On the government side, the methods in place to run systematic data quality processes, range from certification of carriers[143] to checks on data formats[144], data completeness[145], and accuracy[146]. The survey for this Study confirmed these conclusions. The majority of respondents seemed to rely on sanctions as a quality assurance mechanism (10 responding border management authorities); manual review of data (6) and consultations (5). Few relied on automated IT solutions for data quality verifications (4), while one reported a 'dashboard to carriers to monitor their quality'.

The air carriers survey indicated that very few (4 of 20) rely **exclusively on** the OCR for extracting data from the MRZ of travel documents. The methods are usually mixed and include self-declaration of passengers via an app/website (9 of 20), and manual collection by staff (9 of 20). IATA data indicate that 92% of global passengers are offered some kind of self-service check-in option (web, mobile or kiosk), while 57% of global passengers are offered the option to self-board (either by scanning their document or through automatic doors)[147].

Using manual self-declaration methods to capture API data is likely to have a negative impact on data quality, increasing the numbers of false positives in the processing of API data and requiring intensive resources to manually check hits, with a negative impact on travellers.

According to IATA data provided for this Study, an average of 2-10 minutes is spent on manual entry of data, depending on the complexity of data, while a passport swipe of MRZ is typically 20 seconds.

The overall cost/impact on carriers due to the differences observed in enforcement regimes across Europe was revenue lost as a result of financial sanctions and the burden associated with abiding by different rules across the Member States. An estimate of the latter was not gathered during the 2020 evaluation, while the average size of financial sanctions were in the order of EUR 4,000 per breach (i.e. where API transmissions were incomplete or not received by national authorities).

The current process is not efficient for either air carriers or travellers (who spend a longer time on manual check-in), or for government agencies (who rely on sanctions or manual checks).

Coherence

The inconsistencies and shortcomings in the functioning of the API Directive reflect the fact that the Directive is a first-generation legal instrument, which is no longer in line with the latest legal and policy instruments[148]. Air carriers have called for harmonisation of the different national transmission requirements and sanction regimes across the EU Member States. In the absence of harmonised requirements for data quality assurance on both the government and carrier side, data quality, error rates and sanctions vary between Member States, and between carriers.

In respect of quality requirements and assurance mechanisms, as well as sanctions and penalties, there is no coherence between the API Directive, the PNR Directive or the ETIAS Regulation. Firstly, the PNR Directive does not have specific data quality

[143] 2020 evaluation: BG, FR, LU.

[144] 2020 evaluation: BG, PL, SI, CH.

[145] 2020 evaluation: SK, CH.

[146] 2020 evaluation: BG, LT, LV.

[147] IATA data presented for this Study.

[148] 2020 evaluation.

requirements, as PNR data fields are mostly declarative in nature (i.e. not verified by an independent authority). Compliance of the PNR message is assessed in terms of the message format and timing of its transmission. Secondly, the ETIAS Regulation does not impose quality requirements on data capture but, rather, a series of processes contributing to the standardisation of the passenger data sent. The personal data (captured from the MRZ) to query ETIAS/EES (VIS) contain (almost) the same data fields as those captured and transmitted under the API Directive. While Article 45(2) of the ETIAS Regulation refers to MRZ data as part of carriers' interactive query (details of the query to be further outlined in a Commission Implementing Decision), Article 13(3) of the EES Regulation specifies the individual components, corresponding to the MRZ (see section 3.2).

The coherence score for this policy option is assessed as 2/5. Firstly, in terms of internal coherence, the current definitions of sanctions, transmission of API data, or data quality bring little harmonisation across the EU. Secondly, there is no external coherence with ETIAS/PNR rules for data quality when passenger data is captured, nor for related sanctions/penalties, or rules on transmission.

Data protection and fundamental rights

The 2020 evaluation found no evidence of API data processing impinging on the right to free movement of EU citizens. The present level of errors resulting from low data quality may lead to false positives, which may infringe fundamental rights (people stopped or detained at the border) or data protection regulations (false positive information may be retained).

The overall assessment for data protection and fundamental rights is that the current quality assurance processes and systems in respect of collection and transmission of API data do not pose significant challenges to data protection or fundamental rights. Nevertheless, there is room for improvement, as false positives (and retention of such data) may, in certain circumstances, present both a fundamental rights and a data protection issue.

Table 27. Overview of the assessment for policy option IV, baseline scenario

Policy option IV			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	■■■□□
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at the EU external borders	■■■□□
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	■■■□□
	Auxiliary objective	Public health control	□□□□□
Overall effectiveness assessment			■■■□□
Efficiency	***Costs***	Carriers	■■■□□
		Border management authorities	■■■□□
		Law enforcement authorities	■■■□□
	Benefits	Better passenger data	■■■□□
		Better risk analysis	□□□□□

	Better operational planning	□□□□□
	Better operational response	■■■□□
Overall efficiency assessment		■■■□□
Coherence	Streamline API with international standards	□□□□□
	Objectives of the Schengen Borders Code	■■■□□
	Objectives of EES Regulation	■■□□□
	Objectives of ETIAS Regulation	■■□□□
	Objectives of VIS Regulation (and proposed recast)	■■□□□
	Objectives of the Interoperability Regulation	■■□□□
	PNR Directive objectives	■■□□□
Overall coherence assessment		■■□□□
Overall data protection and fundamental rights assessment		■■■■□

3.7.2 Policy option IV, scenario 1: Mandate automated collection of API data and harmonise the sanctions regime

Summary of policy option IV, scenario 1

This scenario considers **mandating automated collection of API data,** i.e. **eliminating manual entry at check-in and online manual self-declaration** of API data by the passenger. This would entail the capture of API data from the MRZ (in conformity with ICAO 9303) through automated means, such as devices using technologies (e.g. OCR, infrared light). The collection of additional information on secondary travel documents (for passengers with dual nationality or where other travel documents have been used, such as residence cards/permits) could also be considered, provided they have an MRZ as per ICAO 9303 standards. Airport check-in processes would include scanning the MRZ of the document at kiosks or by carriers' agents. Online check-in would imply passengers checking-in using electronic devices to scan the MRZ – such solutions are already widely available and implemented by some carriers.

Harmonised and reinforced carrier sanctions

The harmonisation of carrier sanctions across the EU would create equal incentives to improve data quality across the EU. The scenario foresees the establishment of clearer criteria and definition of data quality thresholds, which, if unmet, would result in carrier sanctions. There are currently three grounds for sanctions: data 'not transmitted', 'transmitted incomplete' and 'false data'. None of these categories is defined in sufficient detail or linked to any specific level of sanctions (Article 4(1)(a) and Article 4(1)(b)). A sanction regime needs to differentiate and define 'timely transmission' vs. 'no transmission at all'; completeness of data in terms of missing information on certain passengers, or specific data fields within a passengers' data; 'false data' (due to technical error), e.g. data misread by an OCR device, over-written manually by a carrier representative, or due to passengers holding counterfeit documents. Each of these different possibilities would imply different levels of carrier liability and should have different, proportionate, levels of sanctions.

The sanction regime should be designed according to the actual impact and consequences of failure to comply. Factors for deciding on the level of sanctions are, in decreasing order of importance, data timeliness (allowing border management authorities to process the data and act on suspected individuals), data accuracy[149] (obliging carriers to invest in automated data capture systems), and completeness[150] (missing data fields negatively impact the processing of API data).

The air transport industry has called for a collaborative approach to compliance. Sanctions should be imposed as a last resort and when there is a failure to cooperate. Such an approach should include a feedback process where data errors (including lack of submission and/or receipt) are notified to both the carrier and government as near to real-time as possible to allow for resolution or rectification. The revised API Instrument may allow for different forms of cooperation, while indicating that failure to collaborate would be sanctioned.

Timing of transmission

The **timing of transmission of API** data could be further specified and harmonised across the EU to ensure completeness and maximum accuracy of data. While there are various ways in which the transmission of batch API could be improved and harmonised, the most effective collection of API data is iAPI after check-in of each traveller. This approach would eliminate the need for multiple batch transfers and ensure that API on both outbound and inbound travellers is sent in advance.

iAPI is the only efficient way to ensure sufficient time for processing of API data prior to (most) travellers reaching the border checkpoint. A batch transmission after check-in closure for outbound travel has little or no value for law enforcement or border authorities, as at this point most travellers would already have passed through border control. On the other hand, with a majority of travellers now checking in via mobile or computer-based platforms before the airport check-in process even starts, iAPI would provide sufficient processing time.

Alternatively, batch transmission of API should follow the best practices now observed in many Member States for both inbound and outbound travel – a first batch transmitted at the close of check-in, and a second batch after the aeroplane takes off. Similarly, for other modes of transport, transmitting API batches after the vessel, train, or coach leaves the port or station may make sense.

3.7.2.1 MCA: assessment of effectiveness

The mandatory use of automated processes such as OCR to extract the data from the MRZ is likely to practically eliminate issues linked to accuracy, and, to some extent, completeness of API data. The survey results showed that both border management officials[151] and air carriers overwhelmingly[152] believed that the use of OCR of the MRZ

[149] MRZ detection or character reading accuracy from dedicated scanners at check-in kiosks and counters is close to or at 100%, but this may not always be the case via mobile apps for a number of reasons. 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

[150] Sanctions should still account for the fact that that MRZ captures information via OCR and may still contain errors, either because there were mistakes by the issuer of the travel document, or low OCR accuracy.

[151] 31 of 33 border management and law enforcement authorities surveyed agreed or strongly agreed that automated checks would improve data quality.

[152] Of those familiar with this technological solution, 14 of 15 respondents gave a rating of 5/5 or 4/5 for this solution.

of travel documents is conducive to enhancing the quality of passenger data captured (see Annex 8).

The higher quality of API data transmitted will eliminate the risk of entirely missing advance information on a person who represents a threat and for whom additional analysis could be carried out. This, in turn, would increase the effectiveness of law enforcement and border management authorities in tackling irregular migration, organised crime, and terrorism.

The second effect will be to reduce the number of false positives, i.e. misidentifying travellers who are not a threat. False positives not only waste border guard and law enforcement resources[153], but, in some cases, may impinge on travellers' fundamental rights.

The automated capture of API data, as well as the timing of transmission, would allow law enforcement and border management authorities sufficient time to verify the information and assess if a passenger represents a threat.

The transmission of iAPI after check-in may help law enforcement to preventing passengers who represent a threat from boarding an aircraft or reaching the EU. The 'transmission of a batch of API' or iAPI close-out message is still necessary to improve quality. API data transmission after the departure of the aircraft - for both outbound and inbound flights - has value for border and law enforcement authorities, as it is the only way to be sure of the final list of passengers present on a specific flight. For inbound travel, both iAPI close-out message or 'wheels-up' batch transmission could provide the necessary time to assess risks and facilitate border controls. The outbound travel 'wheels-up' batch transmission has value for law enforcement purposes, as it would constitute confirmation that the traveller actually boarded the flight and could be used for analysis alongside the PNR data received.

The proposed harmonisation of sanction regimes will also contribute to improved data quality by incentivising carriers to invest in automated API data collection (OCR of the MRZ).

The overall assessment is that the proposed scenario would have a positive effect on achieving the objectives of the API Directive. Improving data quality would have a positive effect on the quality of border checks and improve the security of EU citizens by countering the threats of terrorism and irregular migration.

3.7.2.2 MCA: assessment of efficiency

Costs

Transport services operators: The set of processes for capturing API data would impact on their capital and operational expenditure (infrastructure investment, IT costs, modifying and/or adapting operations). Carriers would have to modify and upgrade their existing software and hardware infrastructure (e.g. develop new mobile phone apps, invest in more equipment to read MRZ), modify their operational set-up to allow the capture, aggregation and transmission of passenger information. Web/mobile check-in option is not universally accepted in all countries outside the EU (100% within the EU). Countries representing 95.84% of all global passengers accept mobile check-in – the remaining 4.2% of countries could process documents at the airport check-in desk[154].

Border management authorities: The automation of data capture by carriers will also impact border management and law enforcement authorities. There seem to be differences in the expected costs between two groups of Member States, depending on

[153] The majority of respondents to the law enforcement survey strongly agreed or agreed (9 of 15) that false positives pose a challenge to law enforcement.

[154] Data presented by IATA for this Study.

their current systems. Half of the border management and law enforcement authorities surveyed considered that the automated collection of API data would require modification of their API systems, as well as their messaging and communication systems. The other half did not believe there would be such effects[155]. Timing and sanctions may require administrative and managerial changes.

Law enforcement authorities: Similar types of costs will be incurred to those for border management authorities, depending on the governance arrangements at Member State level.

Travellers: Different technical solutions may accommodate the needs of travellers, allowing them to read the MRZ information contained in their travel document via electronic means. If the range of technologies considered by air carriers is sufficiently open to cater for the different technologies for OCR reading, there will be no added costs to travellers.

The calculated costs across the relevant stakeholder groups are shown below. The full methodology used for the calculation of costs is provided in Annex 6.

Table 28. Overview of costs across stakeholder groups

Stakeholder	**Estimated additional costs (rounded to the nearest million)** ***Scenario 1***
Air carriers	EUR 737.0 million
Border management authorities	EUR 13.0 million
Law enforcement authorities	EUR 13.0 million

Source: ICF estimates

Benefits

Transport services operators: Higher levels of API data quality may result in cost savings for carriers, avoiding multiple transmissions and increasing their legal certainty while reducing their risk of exposure to sanctions for non-compliance. IATA data indicate that swiping a travel document through an OCR reader takes about 20 seconds, compared to 2-10 minutes to manually enter data. This could result in faster processing of aircrafts, fewer delays and shorter times needed to process an aeroplane.

High API data quality reduces carriers' exposure to sanctions (linked to the API Directive) or penalties associated with bringing inadmissible passengers to the country of destination and having to send them back at their own cost.

Border management authorities: The scenario will mainly lead to improvements in the current operations and result in better quality data and harmonisation, including for API data formats. Operational benefits could include better API data matching (i.e. vs. national watchlist), avoidance of false positives, more efficient verification of such cases, more illegitimate travellers barred from boarding, and limiting unnecessary or multiple processing of API data, thereby saving border control resources at the point of arrival.

Law enforcement authorities: Higher levels of data quality would generate several operational benefits, from enhanced threat and risk analysis to intelligence gathering leading to a better intelligence picture, better API and PNR data matching (i.e. vs. national watchlist), and avoidance of false positives.

Travellers: This scenario would have a positive impact on travellers' experiences, with less time spent on the check-in process: either doing a self-check in via a mobile app

[155] See Annex 6.

(data will be extracted automatically, instead of having to enter it manually), or at the check-in counter, where they will processed more quickly.

The overall assessment of efficiency concludes that the benefits of this scenario outweigh the costs. While some airlines and border management/law enforcement authorities may have to make additional investments, they will reap efficiency and effectiveness benefits in their operations.

3.7.2.3 MCA: assessment of coherence

The proposed scenario would primarily contribute to improving the internal coherence of the API Directive. It would harmonise (1) data capture modes (2) sanctions, and (3) timing of data transmission.

Regarding data capture, the proposed scenario would have some impact on coherence in respect to carrier obligations to query the ETIAS, EES, or VIS systems via the carrier gateway. Carriers are supposed to use data from the MRZ to query the gateway to verify that the traveller has the necessary authorisation to travel to the EU (Article 45(2) Regulation (EU) 2018/1240) or VIS Regulation (2021/1134). While none of these regulations mandates the automated query of these databases by carriers, the automated capture of the MRZ data for the purpose of API data submission, will inevitably impact also the use of this data for other purposes.

In respect to sanctions, the proposed harmonisation of sanctions diverges from the approach adopted in the EES, ETIAS, or VIS Regulations, as none of these instruments has harmonised data quality criteria or related sanctions/penalties. Instead, the three regulations (2018/1240) Art. 62, (2017/2226) Art. 48, and (2021/1134) Art. 36 foresee for Member States to lay down the rules on penalties for their infringement of the Regulation.

Therefore the overall assessment is that the proposed scenario would have effect the external coherence with other regulatory instruments, especially ETIAS and VIS.

3.7.2.4 MCA: assessment of data protection and fundamental rights

The automated process of extraction of data from the travel document would have a limited impact on data protection or fundamental rights. In terms of proportionality, the proposed scenario does not expand the range of the data being collected. The data automation process refers to the minimum data already contained in the passport (MRZ) and the necessity to collect such data (assessed under options above). Later in the process, the extraction of the data would take place with the consent of the traveller, who presents the travel document to ground handling staff to extract the data.

The improvement of data quality (fewer error entries) would reduce the number of false positives (and possible retention of such data), positively impacting the fundamental rights of travellers and (possible) data protection issues.

Table 29. Overview of the assessment for policy option IV, scenario 1

Policy option IV, scenario 1			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■■□
		Enhance the security of citizens in the EU	■■■■□
	Specific objectives	Improve border checks	■■■■□
		Facilitate flow of legitimate travellers at the EU external borders	■■■■□
		Combat irregular migration	■■■■□

		Contribute to the fight against serious crime and terrorism	■■■■□
	Auxiliary objective	Public health control	□□□□□
Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	***Costs***	Carriers [EUR 737.0 million]	■■■■□
		Border management authorities [EUR 13.0 million]	■■■□□
		Law enforcement authorities [EUR 13.0 million]	■■■□□
	Benefits	Better passenger data	■■■■■
		Better risk analysis	■■■■□
		Better operational planning	■■■□□
		Better operational response	■■■□□
Overall efficiency assessment			🟦🟦🟦🟦□
Coherence		Streamline API with international standards	■■■□□
		Objectives of the Schengen Borders Code	■■■■□
		Objectives of EES Regulation	■■■□□
		Objectives of ETIAS Regulation	■■■■□
		Objectives of VIS Regulation (and proposed recast)	■■■■□
		Objectives of the Interoperability Regulation	■■■□□
		PNR Directive objectives	■■■□□
Overall coherence assessment			🟦🟦🟦□□
Overall data protection and fundamental rights assessment			🟦🟦🟦□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.7.3 Policy option IV, scenario 2: Verification of legitimate travellers by a carrier representative through the use of information collected via person-document-ticket verification

Summary of policy option IV, scenario 2

The main objective of this scenario is to further ensure the quality and authenticity of MRZ data by mandating carriers to compare it with the information in the travel document's RFID chip. As outlined in policy option IV, scenario 1, while OCR of the MRZ from dedicated scanners at check-in kiosks and counters is close to or at 100%, this may not always be the case via electronic devices for a number of reasons[156]. The quality of MRZ data can therefore be further assured by comparing and extracting the data from the RFID chip. Such extraction technically needs to be preceded by the extraction

[156] See, for instance: Liu, Y., James, H., Gupta, O. and Raviv, D., *MRZ code extraction from visa and passport documents using convolutional neural networks,* 2020, available at: https://arxiv.org/abs/2009.05489l

via reading (OCR or other means) of the MRZ data. This scenario thus builds on Scenario 1. The extraction of the information from the RFID is protected to prevent remote extraction by hackers. For the extraction of the RFID information, the MRZ data serves as a password to read the RFID and verify that the travel document is in the possession of the person extracting the information, including biometric data. The RFID information extraction could be done either by individuals using electronic devices during the check-in process or at check-in counters/kiosks at the airport.

3.7.3.1 MCA: assessment of effectiveness

Scenario 2 builds on scenario 1. In terms of effects on quality, while scenario 1 is expected to have a significant effect on data quality, scenario 2 would authenticate and fully ensure the quality of the API data from the MRZ. The main expected effects are thus the same as in scenario 1:

- Improving the quality of API data transmitted, and eliminating the risk of entirely missing advance information on a person of interest;
- Reducing the number of false positives, i.e. misidentifying travellers as a threat.

Nevertheless, survey respondents have significantly lower expectations in respect of the effects of verification of the RFID chip on API data quality than OCR reading of the MRZ. The process of authenticating the chip information in the travel document is challenging for private software providers, as they need to be able to extract information from all e-Passports issued by all countries worldwide. Several countries, despite issuing e-Passports with a chip, do not publicly share the cryptographic information needed to authenticate the document.

The Public Key Directory (PKD) maintained by ICAO[157] contains Country Signing Certificate (CSC) information from only 75 Country Signing Certificate Authorities (CSCAs). Germany also maintains a Master List of CSCA and contains certificates from 90 countries[158]. Access to this Certificate is needed to validate the authenticity of the document[159]. Under the proposed scenario, even though biographical and biometric data from the travel documents of the majority of travellers to the EU, especially EU citizens, could be extracted. However, authentication can be an issue. The overall assessment is that the proposed scenario would have a positive effect on achieving the objectives of the API Directive. Further improving API data quality would have a positive effect on the quality of border checks and improve the security of EU citizens by contributing to countering threats of terrorism and irregular migration.

3.7.3.2 MCA: assessment of efficiency

Costs

Transport services operators: The proposed scenario of verifying and/or authenticating data collected, as well as using such biometric data to allow passengers to board, may impact on carriers' capital and operational expenditure (infrastructure investments, IT costs, modifying and or adapting operations). Carriers would have to modify and upgrade their existing software and hardware infrastructure (e.g. develop new mobile phone apps, invest in more equipment to read RFID chips), modify their

[157] https://www.icao.int/Security/FAL/PKD/Pages/default.aspx. The majority of countries not publicly sharing their CSCA information are in Africa.

[158] BSI - The German Country Signing Certificate Authority - Root Certificate - CSCA Master List (bund.de)

[159] This mechanism to ensure the authenticity of the document is known as 'passive authentication' and is standardised by ICAO 9303. Passive authentication uses the same process as digital signatures and a chain of trust. The CSC is used to cryptographically sign the Document Signing Certificate, which in turn is used to sign the content of the e-passport and the information contained in the chip.

operational set-up to capture, aggregate and transmit passenger information. Carriers and airports often use multifunctional equipment, which reads both the MRZ and RFID chips, thus avoiding additional costs. However, those incurring such costs would also imply greater operational changes and expenses. Half of the carriers surveyed (10 of 20) were unable to assess the level of operational and technical feasibility of implementing this scenario. The majority of the remainder (7 of 10) indicated a low level of feasibility (1/5 or 2/5).

Border management authorities: The verification of legitimate travel by carriers reading the RFID chip would also impact border management and law enforcement authorities. There are differences in the expected costs between two groups of Member States. Slightly more than half of the border management and law enforcement authorities surveyed believed that RFID verification would also require modification of their API systems, while the rest cited no such effect. Member State respondents were evenly split on their expectations of the cost and operational effects of this scenario on their messaging and communication systems[160].

Law enforcement authorities: The costs for law enforcement authorities would be similar to those for border authorities.

Travellers: Technically, reading of the RFID can be done either at the check-in counter at the airport or via the use of mobile phone with the activation of NFC functionality. This availability of such functionality in mobile phones has increased rapidly in recent years due to its use for e-wallet payments. According to the most recent data, at the end of 2019, 81% of mobile phones had such functionality[161]. Nevertheless, the need for RFID reading limits the check-in options for travellers, computer-based via web may not be possible.

The calculated costs across the relevant stakeholder groups are shown below. The full methodology used for the calculation of costs is provided in Annex 6.

Table 30. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs** (rounded to the nearest million) ***Scenario 2***
Air carriers	EUR 1,447.0 million
Border management authorities	EUR 13.0 million
Law enforcement authorities	EUR 13.0 million

Source: ICF estimates

Benefits:

Transport services operators: Better API data quality might result in cost savings for carriers by avoiding multiple transmissions and increasing their legal certainty, while reducing their risk of exposure to sanctions for non-compliance. High API data quality reduces carriers' exposure to penalties associated with bringing inadmissible passengers to the country of destination and having to send them back at their own expense (especially with the future implementation of the ETIAS/EES/VIS query). Some unintended benefits might be found in reducing the phenomenon of 'ticket swapping' after check-in, which undermines other carriers' fare policies. Transport operators would benefit from passenger facilitation through the use of biometrics (facial image), leading to process improvements for baggage drop, security check and lounge access. Most

[160] See Annex 7.

[161] http://beta.evolita.com/explore/nfc-enabled-smartphones-penetration-rate-worldwide-between-2014-and-2019/5oqme/

importantly, the introduction of scenario 2 biometric-based systems could result in reduced boarding and turnaround times for air carriers.

Border management authorities: Operational benefits could include better API data matching (i.e. vs. national watchlist(s)), avoidance of false positives, illegitimate travellers being barred from boarding, limiting unnecessary or multiple processing of API data and saving border control resources at the point of arrival.

Law enforcement authorities: Higher levels of data quality would generate several operational benefits from enhanced threat and risk analysis, intelligence gathering leading to a better intelligence picture, better API and PNR data matching (i.e. vs. national watchlist) and avoidance of false positives. It would also reduce the time spent on reconciling data during the analysis process.

Travellers: Scenario 2 may have some additional benefits for travellers. In respect of the check-in process itself, there would be no additional benefits compared to scenario 1. If the application of scenario 2 is broadened to 'one ID' type of contactless travel, then the benefit would be an improved journey experience during outbound travel, with reduced time at checking points. From the perspective of health emergencies such as COVID-19, faster processing of passengers could reduce health risks, with the use of the biometric information allowing contactless controls at security, access, or even the border.

Authenticity travel facilitation and using RFID

In addition to benefits linked to quality, scenario 2 could the benefit of establishing legal grounds allowing carriers to use the biometric data from the RFID chip (e.g. facial image) to verify that API data extracted during the (self) check-in process correspond to the passenger boarding the plane (or other mode of transport). This opportunity would open the door to additional benefits, which may not be linked directly to quality. For example, it would improve the identification of passengers, ensuring that documents are genuine and that the document holder is the person checking-in and boarding the aircraft.

Scenario 2 would also open the door to establishing the legal basis for carriers to extract biometric data (e.g. facial) for travel facilitation programmes, such as the IATA 'one ID' concept. The practical implementation of this option would use the digital identity solution and include the (consensual) pre-enrolment of travellers' biometric information. There have been pilot projects at 11 major EU airports (and another 40 major airports internationally).

The basic process of this scenario would typically include two steps: (1) initial online registration or enrolment of the traveller, where the authenticity of their document and their identity is verified with information extracted from their travel document's RFID chip, and (2) subsequent verification of their identity through facial recognition.

There are different modalities and details to implement this process. The initial registration could be done by the air carrier or by travellers themselves at kiosks or via an electronic device. In the case of carrier-run enrolment, the initial registration could rely on existing digital identity verification services, such as e-ID, or other forms of electronic verification, which differ between the Member States.

After the biometric data is extracted from the travel document, it would then be matched against the image of the person enrolled, using either facial recognition software or validated by in-person registration. Once the traveller is registered and enrolled, further verification could take place at the boarding gate, where the identity of pre-enrolled traveller is verified via facial recognition. The possible applications are much larger and could include each point of the airport journey (from the baggage drop-off to security checks and on to the boarding gate), where equipment using facial recognition verifies the identity of the traveller. The privacy and security of the information in such solutions could be protected through GDPR-compliant block-chain technologies[162].

3.7.3.3 MCA: assessment of coherence

The proposed scenario would have some impact on internal and external coherence. In terms of external coherence, it would only build on and strengthen the coherence achieved if scenario 1 is implemented.

The effect on ensuring coherence with PNR/EES/ETIAS would be limited, as none of these instruments has sufficiently defined data quality criteria. As in scenario 1, one area where Scenario 2 could further contribute to improving data quality is querying the ETIAS information system via the CG.

One area that needs to be considered – and where this option would not be coherent – is the security of ID documents mandated in Regulation (EU) 2019/1157. This regulation obliges all ID cards documents issued by Member States to contain MRZ, complying with ICAO 9303. As there is no obligation for such documents to contain an RFID chip, it would not be possible to mandate the collection of API data from the RFID chip for intra-Schengen flights.

3.7.3.4 MCA: assessment of fundamental rights

The basic scenario proposed, i.e. the automated verification of the RFID chip data, does not imply any additional impact on human rights beyond the baseline, as it concerns only information which is already supplied to ground-handling or border authorities. The possible application of RFID data for the purpose of 'seamless travel' solutions, which involve sharing biometric information with multiple stakeholders, may raise privacy and data protection issues. One of the possible mitigation measures that could be used to manage shared use of traveller data by different authorities, while addressing privacy concerns, is blockchain technologies. The key reason to use blockchain is to preserve privacy and limit the sharing of biometric data between the various stakeholders in the airport environment – carriers, ground handlers, security providers, border authorities[163]. The use of block chain 'distributed ledger technology' ensures that no single authority has control over the information shared, while cryptography allows for security in authorisation and sharing of information[164].

As in scenario 1, scenario 2 does not expand the range of the data collected and is therefore proportional, with the need to collect such data long established.

This scenario is assessed as 2/5 because mitigation measures exist for the risks identified. Improvement of data quality would also reduce false positives (and related retention of such data), positively impacting the fundamental rights of travellers and possible data protection issues.

Table 31. Overview of the assessment for policy option IV, scenario 2

Policy option IV, scenario 2			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■■□

[162] European Parliament, *Blockchain and the General Data Protection Regulation,* 2019, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, p.I.

[163] Projects such as the Known Traveller Digital Identity, supported by the World Economic Forum (WEF), is only one example: See WEF, *The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel*, 2018, available at: http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

[164] WEF, 2018, p.5.

		Enhance the security of citizens in the EU	■■■■□
	Specific objectives	Improve border checks	■■■■□
		Facilitate flow of legitimate travellers at the EU external borders	■■■■□
		Combat irregular migration	■■■■□
		Contribute to the fight against serious crime and terrorism	■■■■□
	Auxiliary objective	Public health control	□□□□□
Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	***Costs***	Carriers	■■■■■
		Border management authorities	■■■□□
		Law enforcement authorities	■■■□□
	Benefits	Better passenger data	■■■□□
		Better risk analysis	■■■□□
		Better operational planning	■■■□□
		Better operational response	■■■□□
Overall efficiency assessment			🟦🟦🟦□□
Coherence	Streamline API with international standards		■□□□□
	Objectives of the Schengen Borders Code		■■■□□
	Objectives of EES Regulation		■□□□□
	Objectives of ETIAS Regulation		■■■□□
	Objectives of VIS Regulation (and proposed recast)		■□□□□
	Objectives of the Interoperability Regulation		■□□□□
	PNR Directive objectives		■■□□□
Overall coherence assessment			🟦🟦□□□
Overall data protection and fundamental rights assessment			■■□□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.8 Policy option V: Possible measures on integrating API into the framework for interoperability between EU information systems

This option examines the possibility of streamlining the transfer of API data between carriers and national authorities by reusing the carrier interface defined under the EES(VIS) and ETIAS Regulations[165]. The interactive query foreseen for the ETIAS and EES systems will use (a sub-set of) API data and the air carriers' interactive API IT/communication infrastructure. As a result, the carrier gateway for EES and ETIAS de facto sets a foundation for a centralised point of communication for all air carriers to transmit API data. This introduces new opportunities for optimising the transfer of API data between carriers and national authorities. This could be achieved by having the CG forward API data to the national authorities, enabling them to receive API data before take-off (typically as soon as passengers check-in). The carrier gateway could also collect responses from national authorities and add them to the EES/ETIAS response to the carriers, enabling national authorities to benefit from the features promised by the interactive API systems.

This policy option builds on the conclusions of the feasibility study on a centralised routing mechanism (CRM) (the CRM study)[166], which examined how CRM functionality would modify current API data exchanges via the introduction of a single window[167]. From a technical perspective, the functionality required of both the CRM and the carrier gateway (forwarding EDIFACT/XML messages to the recipients) is identical, thus CRM/carrier gateway are presented as the same element.

3.8.1 Assessment of the baseline+

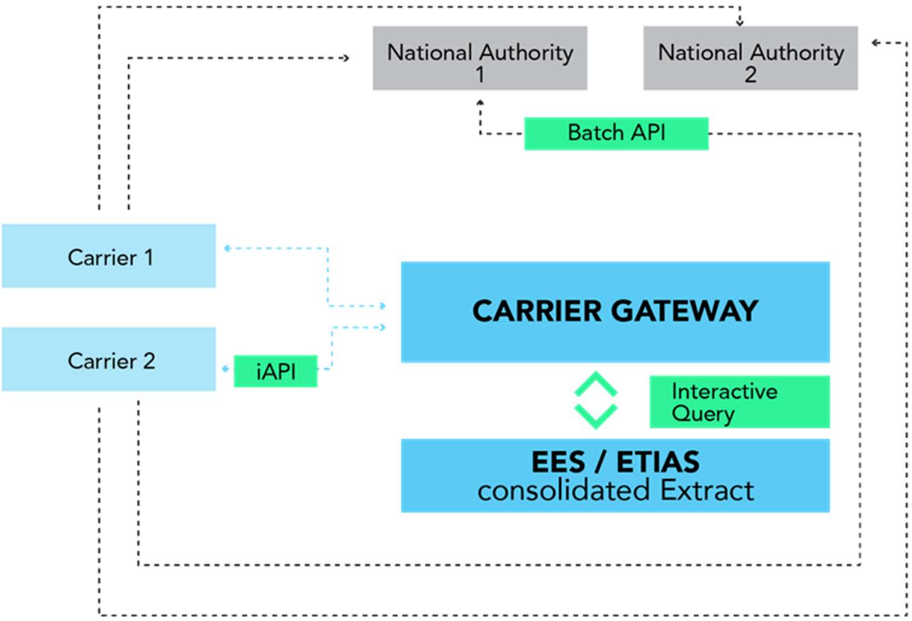
If no other changes are made to API transmission following the introduction of the interactive query to ETIAS and EES (VIS), passenger data will be captured once but will require several transmissions: batch API data will be transferred to the competent authority (or several authorities if no single window approach for receiving API data is established at national level), while an interactive query will be performed against the central systems for EES and ETIAS (Figure 9).

[165] 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; Proposal amending VIS Regulation (COM(2018) 302 final).

[166] https://op.europa.eu/en/publication-detail/-/publication/3ce76d7a-2838-11e9-8d04-01aa75ed71a1/language-en

[167] Carrier gateway is technically intended for all transports. Under the current legal basis the aim would be to make the MSWs interoperable with the carrier gateway. Under an extended legal basis, the CRM/CG could replace the MSWs as the former would forward the API data to NAs.

Figure 9. API transmission in the baseline+ scenario



Source: Unisys

3.8.1.1 MCA: assessment of effectiveness

Carriers are obliged to manage the distribution of API data to all requesting authorities in different data formats and at different times. In order to receive data from carriers, Member States must engage with each carrier and their DCS provider separately. Adding a new interactive query for EES and ETIAS without consolidating existing API transmission would not be welcomed by carriers: they expect batch API transfers to cease once iAPI commences, with the CRM/carrier gateway as a single window for all EU passenger data exchanges. The CRM/carrier gateway would thus have to facilitate delivery of API to the Member States.

In addition to the unnecessary complexity of the API data transmission infrastructure between carriers and national authorities, the API information in the baseline scenario also does not help carriers prevent the boarding of inadmissible and unwanted passengers. Carriers have to maintain manual processes at the departure to perform verifications that could easily be performed by national authorities systems using the API data. This is due to the fact that Member States receive API information about passengers in advance of their arrival but not necessarily in advance of their departure. More specifically, API data sent at close of boarding or at the time of departure does not allow sufficient time to have an inadmissible passenger (for immigration or security reasons) removed from the flight. As a result, there is a missed opportunity for carriers to leverage the national authorities systems to verify passenger admissibility.

While the interactive query against EES and ETIAS seeks to provide carriers with timely advice on whether or not a passenger has the appropriate travel authorisation to enter the Schengen area, it only covers part of the potential travel screening. It does not cover interactive pre-departure checks for security or customs purposes for all passengers[168]. This is in contrast to the iAPI implementation in other countries, where secondary processing usually includes such checks.

This serves to illustrate the need for rationalisation of API data transfers, which would reduce costs and effectively reallocate resources engaged in border management. Lack of an integrated approach to API transmission hinders the optimal protection of EU external borders and enhanced security of its citizens. Some stakeholders noted that retaining the current status would avoid the risk of disrupting satisfactory operational systems. However, simplification of data flows (through an SW) and standardisation would facilitate the flow of legitimate travellers at EU external borders. At the same time, comprehensive responses to carriers' queries (i.e. responses combining the EES/ETIAS OK/NOK status with additional indicators resulting from watchlist checks done by the national authorities) would help to combat irregular migration and contribute to the fight against serious crime and terrorism and even public health control.

The overall effectiveness of the baseline is therefore considered as below average, considering the opportunities available by carriers to check passenger before departure and the complexity, created by the API data transmission point to point infrastructure combined with the local variations of message timings and content, impede the evolution of API usage within the EU.

Efficiency

The carrier interface could evolve naturally to support batch API and transmit them to national authorities[169]. The existing infrastructure could be adapted by adding a routing task that is not built-in from the start.

In this baseline scenario, the interactive query against the EES and ETIAS central systems is an additional requirement imposed on carriers. The carriers now have to send normalised interactive API data centrally, and continue to maintain the existing connections to the national authorities to resend the same data in batch form with some form and content variations between national authorities.

The lack of a holistic view of API data transfer prevents carriers and competent national authorities from benefitting from the single window approach. Standardisation of formats and timing would result in better passenger data, while the features of the carrier gateway would enable better risk analysis, better operational planning and responses. Carriers' use of iAPI (similar content to batch information) results in API data being sent to the carrier interface. Thus, the opportunity to forward API to national authorities should be used, simplifying the carriers/national authorities' connectivity infrastructure.

The complexity of the API transmission infrastructure and variations in data exchange arrangements between carriers and National Authorities lead to a low efficiency of the current technical ICT aspects of the baseline. The low ICT efficiency does not however directly impact the business operations so the overall efficiency is considered below average.

Coherence

This scenario is coherent with the API and PNR Directives, the EES/ETIAS Regulations and the Schengen Borders Code. It is not, however, in line with the Passenger Data Single Window facility listed as recommended practice in Annex 9 to the Chicago Convention. According to Recommended Practice 9.17, an iAPI should be integrated

[168] Exemptions referred to in Art 2(3) of ESS and Art. 2(2) of ETIAS Regulations. The recast VIS Regulation (Regulation (EU) 2021/1134)increased the coverage (with the introduction of Art. 45c, third country nationals who are required to hold a long-stay visa or residence permits are also added) but a number of gaps remain, notably residence cardholders and the several exempt categories (e.g. diplomats, royal family members, merchant seamen, etc.).

[169] Interview with an EU agency.

with an ETS. This would allow States to integrate with the airline DCS' using data messaging standards in accordance with international guidelines, providing a real-time response to the airline to verify the authenticity of passengers' authorisation during check-in.

Nor is this scenario in line with Recommended Practice 9.10 of Annex 9 to the Chicago Convention, which suggests minimising the number of times API data are transmitted.

Finally, it does not comply with Recommended Practice 9.8 of Annex 9 to the Chicago Convention, which requires that only the limited sub-set of identification data (data elements available in the MRZ, in line with the specifications contained in ICAO 9303[170]) should be requested.

This scenario does not consider all the possibilities for avoiding multiple transfers of same data made possible with the Interoperability Regulation.

Following the points above the baseline coherence assessment is low for addressing the streamline API with international standards and the oobjectives of the Interoperability Regulation.

Data protection and fundamental rights

Once ETIAS and EES implemented, personal data will be processed many times when sending it to multiple authorities and systems, which could call into question the compliance of this state of play with certain data protection principles. In addition, at present, the API Directive allows Member States to request more data from carriers than is necessary (e.g. the limitation to MZR data fields as per Annex 9 to the Chicago Convention is not observed).

The current situation entails data quality issues compared to countries that support interactive processes to automate the validation by carriers of travel documents against national authorities records of authorised passengers. Airline practice is currently such that data validation is limited to checking the validity of dates. Additional features could be enabled to do so by some operators but this would mean an increase in boarding time as all travel documents would need to be swiped, including transfer passengers.

Some key points of the privacy impact assessment are:

Favourable impacts	Unfavourable impacts
• Consequences of security incidents are limited to a connection to a single Member State. Connections to other Member States remain unaffected. • No need for a central hosting authority with the possibility to access data by virtue of technically administering the systems. However, a system administration function also exists for connections per individual Member State.	• Increased risk of unauthorised access due to multiplicity of open network (i.e. internet) connections. • Smaller Member States have to deal with the burden of data monitoring in terms of security.

[170] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

Table 32. Overview of the assessment for policy option V, baseline scenario

Policy option V, baseline scenario			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■□□□
		Enhance the security of citizens in the EU	■■□□□
	Specific objectives	Improve border checks	■■□□□
		Facilitate flow of legitimate travellers at the EU external borders	■■□□□
		Combat irregular migration	■■□□□
		Contribute to the fight against serious crime and terrorism	■■□□□
	Auxiliary objective	Public health control	■■□□□
Overall effectiveness assessment			■■□□□
Efficiency	***Costs***	Carriers	■■□□□
		Border management authorities	■■□□□
		Law enforcement authorities	■■□□□
	Benefits	Better passenger data	■■□□□
		Better risk analysis	■■□□□
		Better operational planning	■■□□□
		Better operational response	■■□□□
Overall efficiency assessment			■■□□□
Coherence	Streamline API with international standards		■□□□□
	Objectives of the Schengen Borders Code		■■■□□
	Objectives of EES Regulation		■■■□□
	Objectives of ETIAS Regulation		■■■□□
	Objectives of VIS Regulation (and proposed recast)		■■■□□
	Objectives of the Interoperability Regulation		■□□□□
	PNR Directive objectives		■■■□□
Overall coherence assessment			■■□□□
Overall data protection and fundamental rights assessment			■■□□□

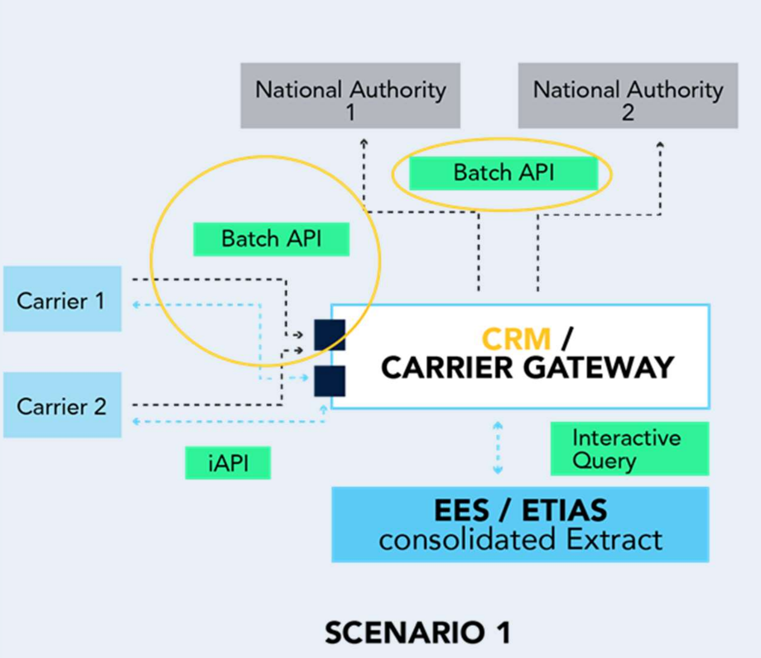
3.8.2 Policy option V, scenario 1: Streamline API data flow

Summary of policy option V, scenario 1

- This scenario considers upgrading the carrier gateway (CG) with the CRM technical capabilities, allowing carriers to send API data to national authorities through a central point following the single window (SW) approach.
- The API information sent via the iAPI protocol will query a consolidated read-only database extracted from EES/ETIAS, as defined in the baseline scenario (see section 3.8.1). An 'OK/NOT OK' response will be routed back to the carrier. Where a passenger does not appear in either of the consolidated databases (i.e. EU citizens), a 'not

applicable' message will be delivered. In addition, the same API data are sent to the carrier gateway for further routing, an element that differentiates this scenario from the baseline and establishes a centralised EU approach for the transmission of batch API data to national authorities:

Figure 10. API transmission in policy option V, scenario 1



Source: Unisys

3.8.2.1 MCA: assessment of effectiveness

The SW for carriers would bring operational rationalisation while facilitating current API batch transfers. It would reduce the complexity for carriers to maintain connections with all EU/Schengen States border management authorities, introduce economies of scale, and enable national authorities to increase the capacity required for API data processing and analysis[171]. This would generally improve border checks and facilitate legitimate traveller flows while contributing to the fight against irregular migration, serious crime and terrorism.

In addition to the simplification of data collection and transfer, other potential benefits could be brought by the wide range of the carrier gateway features for an improvement of the effectiveness of the baseline scenario:

- 24/7/365 support for all Member States offered by the carrier gateway;
- Responsibility of the carrier gateway for monitoring API data feeds against agreed Service Level Agreements (SLAs), using, for example, real-time flight data. The outsourcing of data delivery and basic quality assurance checks would leave Member States free to focus on the content and analysis of API data.
- Possibility for a carrier gateway to monitor the quality of data passing through the system and for statistics to be gathered in preparation for actions to be taken with carriers, where necessary. CRM/CG would carry out basic data quality checks only, as it would not assess the content of the data, but only structure and syntax.

[171] The Member State consultation in the CRM study revealed that of the three Member States sharing resourcing levels, on average one full-time employee supported 15 carriers.

- The carrier gateway might be beneficial for smaller carriers that cannot provide the required resources to support connection with all the Member States.

3.8.2.2 MCA: assessment of efficiency

The scenario improves the efficiency of the business benefit by introducing the single window concept and setting a foundation for aligning standards for passenger data and operational procedures. The technical simplifications brought by the single windows reduce the barrier of entry for the participation of new carriers, resulting in more passenger data and, as a result better overall risk analysis.

For carriers, the scenario would entail costs related to decommissioning some communication links with Member State systems and to training staff on new procedures.

For border management and law enforcement authorities, this scenario might entail some costs related to investment or modification of communication links with eu-LISA. However, it can be assumed that most Member States already have existing communication infrastructures and equipment in place to communicate/deal with eu-LISA. Operational costs are likely to be neutral as staff managing communication links with carriers would be accustomed to receiving data from eu-LISA CG, quality assurance and would have relationships with carriers.

Staff in EU agencies might increase as a result of performing tasks for the EU SW.

The main benefit determining the efficiency of this scenario is the reduction of costs for carriers and national authorities related to the management of multiple connections. This task would be transferred to eu-LISA), centrally hosting the CRM/CG as a single interface to which carriers and national authorities would be connected in order to receive information. Both border management and law enforcement authorities could then reallocate resources to improve operational planning, risk assessment, and operational responses. As the use of batch API data would remain the same, no major investment would be needed at protocol or file transfer level.

The calculated costs across the relevant stakeholder groups are shown below (see **Annex 6** for detail on methodology and costs).

Table 33. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs**
	Scenario 1
Air carriers	0
Border management authorities	0
Law enforcement authorities	0
eu-LISA	EUR 9.5 million

Source: ICF estimates

3.8.2.3 MCA: assessment of coherence

This scenario is coherent with the existing legislative framework in that it would streamline the provisions of ETIAS/EES (and recast VIS) Regulations related to reuse of the carrier interface. Specific reference is made to the Schengen Borders Code in the EES Regulation, on the prohibition to take a decision with significant effects on a person based solely on automated processing (the ultimate decision to allow/refuse entry to the Schengen area should be made by an authority empowered by national law, i.e. by the border guard). It also considers the provisions of the API Directive and (where relevant) the PNR Directive.

The scenario considers four pieces of relevant EU law, coherently providing for principles to be respected in the course of data processing, and which would have to be embedded in the set-up of the CRM/CG:

- Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union;
- Law Enforcement Directive (EU) 2016/680;
- GDPR;
- Regulation (EU) 2018/1725[172], which applies to data processing by EU institutions, bodies, offices and agencies. As such, it would be applicable to eu-LISA, under the assumption that it develops and operationally manages the CRM/CG;
- International standards and guidelines, such as WCO/IATA/ICAO Guidelines on Advance Passenger Information[173] or Annex 9 to the Chicago Convention, which lists a Passenger Data Single Window facility as a recommended practice.

3.8.2.4 MCA: assessment of fundamental rights

The privacy impact assessment in the CRM study[174] concluded that the CRM/carrier gateway solution would comply with the purpose of simplifying the transmission of API data required under the API Directive. It could be seen as an effective tool for facilitating data transmission, with positive implications for both carriers and Member State authorities. The solution would not present more risks to data subjects than the current situation, and opportunities to compromise data while in the queue would be low where strong access control and audit logs are implemented. Please note that this scenario is not considering a reply but only data transmissions through a central point.

The privacy impact assessment of centralised routing for batch API showed that:

- Justification of API transmission is unchanged;
- Data volumes are unchanged;
- Risks of disclosure/unauthorised access to data are unchanged;
- CRM/CG does not contain persistent storage and thus does not create new elements of intrusion in privacy;
- CRM/CG increases consistency and control on the implementation of data protection measures compared to the current situation.

Table 34. CRM/carrier gateway privacy CG privacy compliance for API batch transmissions

Principle	Safeguards
Lawfulness, fairness and transparency	Processing necessary to pursue a legitimate interest: to ensure efficient transmission of API data from carriers to Member States for defined purposes Processing based on EU law (API Directive and relevant amendments, GDPR, Regulation (EU) 2018/1725, Article 77 Treaty on the Functioning of the European Union (TFEU))

[172] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018.

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

[174] The Privacy Impact Assessment in the scope of CRM study included data protection assessment and can be found here: https://op.europa.eu/en/publication-detail/-/publication/42b788e6-2836-11e9-8d04-01aa75ed71a1/language-en/format-PDF/source-search (the last report at the end).

Principle	Safeguards
Purpose limitation	CRM/CG limited to routing messages to the relevant national authorities
Data minimisation	No additional data elements are collected compared to a harmonised and closed list of API data
Accuracy	CRM/CG will run basic data quality checks and maintain statistics for data monitoring CRM/CG is not intended to interpret or transform the personal data contained in the message: there are no checks on accuracy on personal data
Storage limitation	No persistent data storage. The retention period is zero days
Integrity and confidentiality	CRM/CG will have an Identity Access Management (IAM) system in order to control the authentication and authorisation access policy Predefined rules for forwarding messages to Member States: messages to be routed to the appropriate destination based on the values of system configuration parameters Encrypted network links
Accountability	Audit trail to ensure traceability of the origin of queries to the carrier gateway Access and process logging

While facilitating current API data transmissions, the CRM/CG would process large amounts of personal data. The assessment suggests that it is possible to justify the necessity and proportionality of setting up a central routing for forwarding API data messages to Member States: no personal data would be stored persistently within the CRM/CG, minimising the intrusion. Finally, issues related to the security of the data could be addressed by adequate safeguards and mitigation measures.

Table 35. Overview of the assessment for policy option V, scenario 1

Policy option V, scenario 1			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■□□
		Enhance the security of citizens in the EU	■■■□□
	Specific objectives	Improve border checks	■■■□□
		Facilitate flow of legitimate travellers at the EU external borders	■■■□□
		Combat irregular migration	■■■□□
		Contribute to the fight against serious crime and terrorism	■■■□□
	Auxiliary objective	Public health control	■■■□□
Overall effectiveness assessment			■■■□□
Efficiency	***Costs***	Carriers	N/A
		Border management authorities	N/A
		Law enforcement authorities	N/A

	eu-LISA	🟨□□□□
Benefits	Better passenger data	🟦🟦🟦🟦□
	Better risk analysis	🟦🟦🟦□□
	Better operational planning	🟦🟦🟦□□
	Better operational response	🟦🟦🟦□□
Overall efficiency assessment		🟦🟦🟦□□
Coherence	Streamline API with international standards	🟦🟦🟦🟦□
	Objectives of the Schengen Borders Code	⬛⬛⬛□□
	Objectives of EES Regulation	⬛⬛⬛□□
	Objectives of ETIAS Regulation	⬛⬛⬛□□
	Objectives of VIS Regulation (and proposed recast)	⬛⬛⬛□□
	Objectives of the Interoperability Regulation	🟦🟦🟦□□
	PNR Directive objectives	⬛⬛⬛□□
Overall coherence assessment		🟦🟦🟦□□
Overall data protection and fundamental rights assessment		🟦🟦🟦□□

Legend

⬛ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

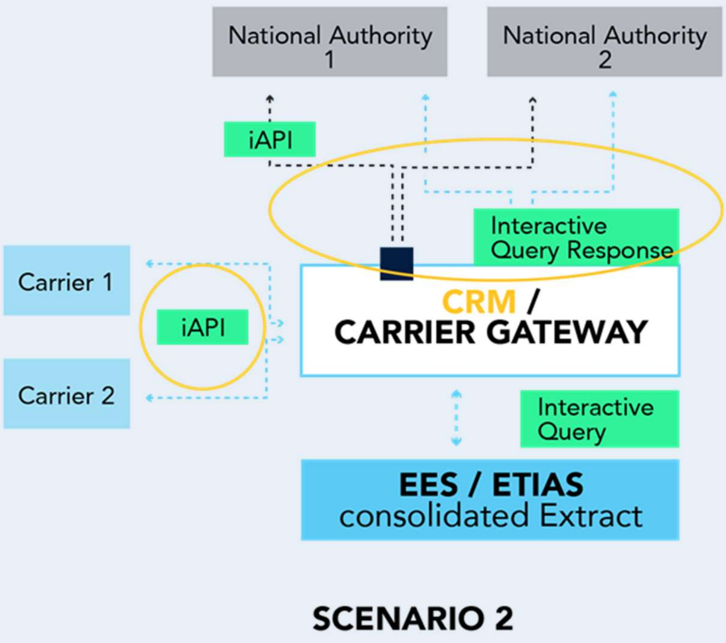
🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.8.3 Policy option V, scenario 2: Merge API and iAPI transfers

Summary of policy option V, scenario 2

- This scenario examines the possibility of transmitting API data to national authorities at the same time as it is received for the query of the EES/ETIAS database (typically at the moment of check-in).
- It further supports the SW approach by enabling API data transfer through the CRM/CG using a single protocol (iAPI) and timing (during check-in).
- This scenario builds on policy option V, scenario 1, considering it implemented to allow for a transition during a set time-period.
- A query containing API data is sent via iAPI protocol to both EES/ETIAS central systems and to national authorities, which receive a response to the interactive query (OK/NOT OK).

Figure 11. API data transmissions in policy option V, scenario 2



Source: Unisys

3.8.3.1 MCA: assessment of effectiveness

As this scenario further consolidates existing API transmission, the benefits related to operational rationalisation described in section 3.8.2.1 also apply here. Indeed, removal of batch API data routing to Member State systems addresses concerns expressed by carriers[175] as to streamlining of timings and formats (PAXLST versions) for exchanges to avoid sending the same data multiple times and in different formats to different recipients. As for API, the iAPI protocol includes a message sent at the time of the flight departure indicating the number of passengers onboard at flight closure.

On the other hand, it would introduce benefits for national authorities in facilitating pre-departure checks for border control and security purposes. The baseline scenario in policy option V does not include national systems in the interactive exchanges, meaning that checks against security databases using API data (national and international) only take place after departure. This would preclude Member States making decisions on allowing passengers to board, which may hinder efforts to combat terrorism and organised crime. Full, advanced vetting of passengers bound for the Schengen border (either entering or exiting) prior to departure requires API data to get to the Targeting Units/PIUs in a timely manner. Copying the iAPI messages to these units would enable this objective to be pursued.

The enablement of pre-departure checks therefore significantly improves the effectiveness assessment score for all the objectives related to border management and security.

[175] Extensive consultations with carriers' representatives were held in the course of the CRM study.

3.8.3.2 MCA: assessment of efficiency

Apart from the costs described in policy option V scenario 1, investments for subscribing, consolidating and routing iAPI data flows from eu-LISA to national level need to be considered.

Scenario 2 would generate cost savings for transport operators due to the removal of sending batch data. Doing away with complying with divergent obligations imposed by national laws would reduce costs and inherent risks of non-compliance. Providing a standard list of API data (as established in the scope of the interactive query) once (single link to the CRM/CG) in a standard format (PAXLST) and following the standard timing (during check-in) would optimise carriers' operations and resources. Standardisation would, in turn, contribute to higher data quality (e.g. use of MRZ data fields) and its monitoring.

National authorities would also be provided with the possibility to stop people of concern from boarding an aeroplane by giving more time to border guards to take appropriate actions. This could enhance border security, speed-up border checks, reduce queuing time for third-country nationals, and, ultimately, have wider economic and social impacts. Border management authorities would have more time to check API data against national databases[176], allowing them additional hours to organise and/or expedite checks at external borders[177]. They could also focus on their core task of data processing and risk assessment. The scenario thus facilitates passenger clearance and might provide a measurable improvement in passenger processing time on arrival and departure. National authorities would have the opportunity to optimise data accuracy by making use of the iAPI functionality. As a result, there is a significant improvement in the efficiency in terms of improved risks analysis and operational planning and response capabilities.

Finally, the scenario builds on the EES/ETIAS carrier gateway as an IT communication stepping-stone to streamline existing API data flows between carriers and national authorities and enable optional transition to iAPI for interested national authorities.

The calculated costs across the relevant stakeholder groups are shown below (see Annex 6 for detail on methodology and costs).

Table 36. Overview of costs per stakeholder group

Stakeholder	Estimated additional costs *Scenario 2*
Air carriers	(-) EUR 95.0 million (cost savings)
Border management authorities	0
Law enforcement authorities	0
eu-LISA	EUR 893,000

Source: Unisys estimates

3.8.3.3 MCA: assessment of coherence

The legislative framework discussed in Section 3.8.2.3 is also relevant here, including the international standards and guidelines (e.g. Annex 9 to the Chicago Convention which identified the use of iAPI systems as a recommended practice)[178]. This leads to an improved score for the coherence with international standards.

[176] This will add value as not all information on suspicious individuals is entered into SIS.
[177] Carriers could further benefit from having their travellers cleared seamlessly at external borders.
[178] Recommended Practice 9.14.

In addition to the three pieces of relevant EU law, which coherently provide for principles to be respected in the course of data processing, the LED should also be mentioned in that it aims to protect the fundamental right to data protection wherever personal data are used by police and criminal justice authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, including the offences covered under the PNR Directive.

3.8.3.4 MCA: assessment of fundamental rights

Even though the proposed approach to transmit API data to national authorities via iAPI protocol broadens the scope of the legal basis of in the EES/ETIAS, it would not change how the CRM/CG would function[179] or how data are processed by the Member States: they already get all of the data that the CRM/CG could provide. No central personal data storage, merge or analysis is envisaged in this scenario. Operational rationalisation would therefore be achieved with little or no impact on privacy related to the possibility of unauthorised access to data, which remains at a technical level only, as no right would be given to access the data processed in the CG or even associated metadata without the authorisation of the data controller. That risk is offset by the gains in increased security. Issues related to the security of the data during the transient data storage remain the same as in policy option V scenario 1, which could be addressed through adequate safeguards and mitigation measures.

Table 37. Overview of the assessment of policy option V, scenario 2

Policy option V, scenario 2			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	■■■■□
		Enhance the security of citizens in the EU	■■■■□
	Specific objectives	Improve border checks	■■■■□
		Facilitate flow of legitimate travellers at the EU external borders	■■■■□
		Combat irregular migration	■■■■□
		Contribute to the fight against serious crime and terrorism	■■■■□
	Auxiliary objective	Public health control	■■■□□

[179] The analysis with regard to the principles of necessity and proportionality carried out in the course of the CRM study was based on the comparison of favourable and unfavourable elements in terms of data protection which showed that a) By virtue of the existence of multiple links (one per carrier/MS combination), the consequences of a data protection breach are fewer than when a CRM/CG solution is used, simply because less data is potentially affected. And b)However, by virtue of the existence of fewer links, the data protection measures – which are not inherently different – can be better enforced and controlled with a CRM/CG solution than with a point to point solution.

The main privacy concerns relate to data availability risks and the possibility to access data by virtue of technically administering the CRM/CG by certain roles within the hosting authority. However, such a possibility exists also currently, only at a local level (i.e. administering connections per individual MS). In any case, these unfavourable impacts on privacy should be mitigated by adequate mitigation measures. On the other hand, the scenario presents advantages as compared to the current situation with regard to the possibility to use the private network instead of Internet, assisting MS in data monitoring activities and ensuring improved integrity and confidentiality of data. In view of these favourable aspects and considering the fact that there is no persistent data storage creating the risk of analysing the data, the level of intrusiveness from the privacy point of view is not increased as compared to the current situation. With intrusiveness of API data transmissions remaining the same, the data protection side offers more guarantees on consistency of implementation.

Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	***Costs***	Carriers	■■□□□
		Border management authorities	N/A
		Law enforcement authorities	N/A
		eu-LISA	🟧□□□□
	Benefits	Better passenger data	🟦🟦🟦🟦□
		Better risk analysis	🟦🟦🟦🟦□
		Better operational planning	🟦🟦🟦🟦□
		Better operational response	🟦🟦🟦🟦□
Overall efficiency assessment			🟦🟦🟦🟦□
Coherence	Streamline API with international standards		🟦🟦🟦🟦□
	Objectives of the Schengen Borders Code		■■■□□
	Objectives of EES Regulation		■■■□□
	Objectives of ETIAS Regulation		■■■□□
	Objectives of VIS Regulation (and proposed recast)		■■■□□
	Objectives of the Interoperability Regulation		🟦🟦🟦□□
	PNR Directive objectives		■■■□□
Overall coherence assessment			🟦🟦🟦□□
Overall data protection and fundamental rights assessment			🟦🟦🟦□□

Legend

■ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

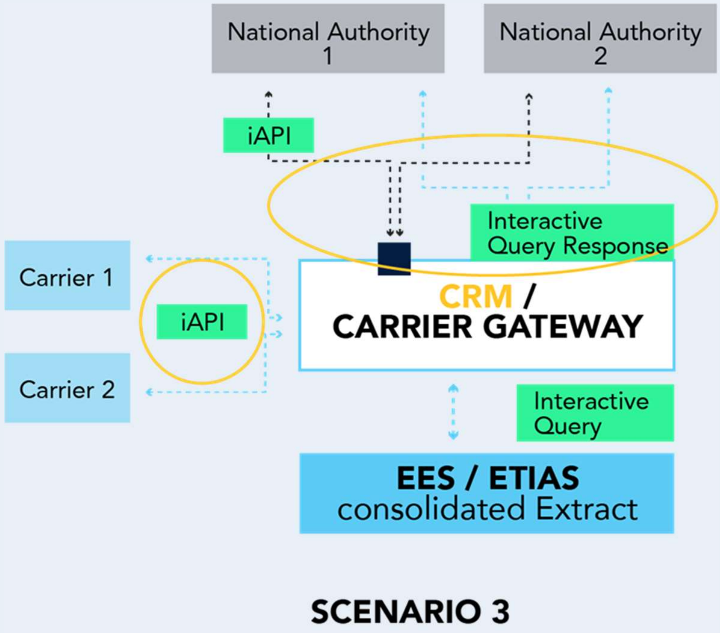
🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.8.4 Policy option V, scenario 3: Complement

Summary of policy option V, scenario 3

- This scenario examines the possibility of enabling Member State systems to complement the iAPI return message (CUSRES) to carriers by sending a response based on the outcome of processing by national authorities, beyond ETIAS/EES checks.
- The Member State receiving the iAPI data could complement an interactive reply – within a 4-second window – using information found in national databases, such as watchlists, to allow or deny entry of a third-country national.
- This scenario builds on policy option V scenario 2, further enabling carriers to receive a comprehensive response on third country national travellers' status prior to boarding.

Figure 12. API transmission in policy option V, scenario 3



Source: Unisys

3.8.4.1 MCA: assessment of effectiveness

As this scenario would further consolidate existing API transmission, the benefits related to operational rationalisation described in sections 3.8.2.1 and 3.8.3.1 also apply here.

In addition, an automated response to the carrier would be generated as a result of security screening based on the data provided in the CUSRES message. National authorities could thus save the time spent informing carriers of identified risks via the competent authorities in the third country. This would facilitate decisions in advance of passengers' departure and close a gap in the security screening. For instance, National authorities could check passenger against their own watch lists and respond immediately (within the iAPI 4 seconds). More sophisticated and time-consuming risk analysis would have to report their findings via other channels, but would still get the opportunity of detecting a risk passenger before boarding.

Overall, the effectiveness is equivalent to Scenario 2 that already leverages the benefits of pre-departure checks on the effectiveness of border management and security objectives.

3.8.4.2 MCA: assessment of efficiency

The capital expenditure implied by this scenario would include adaptations to process complementary messages (if any) and possible upgrades of links to support timely response time (the 4-seconds imposed by the iAPI standard based on common industry practices), with the following implications for border management and law enforcement authorities:

- Cost of setting up the interactive response with complementary messages;
- Investment to ensure timely processing of complementary messages within the required window;
- Investment or modification of communication links between national SWs and eu-LISA to support the required response time.

This scenario supports efficiency as carriers could receive a complementary response from national authorities, allowing for a more informed decision on whether to allow/deny boarding, using the same iAPI.

The interactive approach for advanced vetting of passengers bound for the Schengen border (either entering or exiting) prior to departure via the CRM/CG would be beneficial both from a carrier and Member State point of view. It would include the security dimension in the iAPI response, preventing inadmissible passengers being transported to the Schengen border with the implications for associated support, return, and potential penalties. This would represent significant advantages for carriers' implementing iAPI. Member States would equally benefit from a fuller picture on the status of a passenger due to the proposed secondary processing, which would strengthen security and reduce costs related to controls at border crossing points.

Finally, the possibility to opt to participate in iAPI for security purposes provided to Member States by the fully interactive model could prompt rationalisation of its API infrastructure in a consolidated iAPI/API upgrade project. Such consideration is supported by the cost analysis performed in the scope of the CRM study, which revealed that the overall incremental costs for enabling CRM/CG as an extension to the CRM/CG for iAPI are relatively low (13% of increase related to the baseline total estimated costs[180]). The costs would be incurred by eu-LISA, as they are mainly related to the system infrastructure or operations.

The scenario has the following implications:

- Member State systems would need to be adapted to achieve an interactive 4-second response window to send back complementary messages to the carriers, via the CRM/GW;
- CRM/GW mechanism would need to be adapted to ensure that a 4-second window can be respected in order to timely process complementary messages to the carriers.

The calculated costs across the relevant stakeholder groups are shown below (see Annex 6 for methodology and cost detail).

Table 38. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs** ***Scenario 3***
Air carriers	0
Border management authorities	EUR 2.5 million (across all Member States)
Law enforcement authorities	EUR 2.5 million (across all Member States)
eu-LISA	EUR 982,300

Source: ICF estimates

3.8.4.3 MCA: assessment of coherence

The legislative framework discussed in above is also relevant here.

[180] CRM study, resource requirements (U2-L1-sc10H-DOC-008), page 12.

3.8.4.4 MCA: assessment of fundamental rights

Even if the proposed approach to add national authorities' responses broadens the scope of scenario 2, it would not change how the CRM/CG would function or the way data are processed by the Member States and carriers: no central personal data storage, merge or analysis are envisaged. Issues related to the security of the data during the transient data storage would be similar to scenario 2 and would be addressed by adequate safeguards and mitigation measures.

Table 39. Overview of the assessment for policy option V, scenario 3

Policy option V, scenario 3			Score
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	🟦🟦🟦🟦□
		Enhance the security of citizens in the EU	🟦🟦🟦🟦□
	Specific objectives	Improve border checks	🟦🟦🟦🟦□
		Facilitate flow of legitimate travellers at the EU external borders	🟦🟦🟦🟦□
		Combat irregular migration	🟦🟦🟦🟦□
		Contribute to the fight against serious crime and terrorism	🟦🟦🟦🟦□
	Auxiliary objective	Public health control	🟦🟦🟦□□
Overall effectiveness assessment			🟦🟦🟦🟦□
Efficiency	***Costs***	Carriers	N/A
		Border management authorities	🟧□□□□
		Law enforcement authorities	🟧□□□□
		eu-LISA	🟧□□□□
	Benefits	Better passenger data	🟦🟦🟦🟦□
		Better risk analysis	🟦🟦🟦🟦□
		Better operational planning	🟦🟦🟦🟦□
		Better operational response	🟦🟦🟦🟦□
Overall efficiency assessment			🟦🟦🟦🟦□
Coherence		Streamline API with international standards	🟦🟦🟦🟦□
		Objectives of the Schengen Borders Code	⬛⬛⬛□□
		Objectives of EES Regulation	⬛⬛⬛□□
		Objectives of ETIAS Regulation	⬛⬛⬛□□
		Objectives of VIS Regulation (and proposed recast)	⬛⬛⬛□□
		Objectives of the Interoperability Regulation	🟦🟦🟦□□
		PNR Directive objectives	⬛⬛⬛□□
Overall coherence assessment			🟦🟦🟦□□
Overall data protection and fundamental rights assessment			🟦🟦🟦□□

Legend

⬛ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

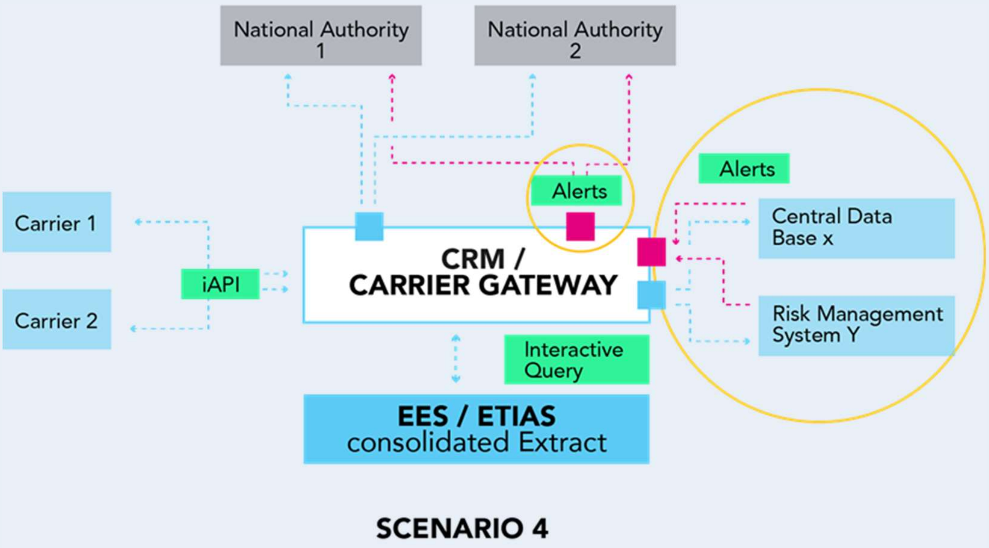
🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

3.8.5 Policy option V, scenario 4: Interoperate

Summary of policy option V, scenario 4

- This scenario proposes an interoperable platform for future passenger validation policies based on API data and central databases.
- It considers the use of the centralised API flow via the CRM to query central databases other than EES and ETIAS, and to complement the API information sent to national authorities with alerts generated from checks on EU and international databases (SIS, EMS, SLTD). For example, once the European Search Portal (ESP) becomes available, the API could be used to perform adequate searches and forward the findings to the relevant national authorities.
- The scenario also considers a generic interoperable mechanism for API data to interact with central risk-analysis systems and leverage data analytics to get an EU-wide picture of API data streams.
- The scenario proposes using API data in the context of a long-term evolution towards a centralised risk management and border control decision support toolset resulting from combining interoperable API data and interoperable central databases services.

Figure 13. API transmission in policy option V, scenario 4



Source: Unisys

3.8.5.1 MCA: assessment of effectiveness

This scenario would make API data available in an interoperable way to all central applications and/or databases that require passenger data to achieve their business purposes (advanced compliance checks and/or targeting) as these systems become available. The CRM/CG would also be used to forward the results to the appropriate national authorities based on API data routing rules. For checks in SIS, the approach would provide added value for Member States that do not have a national copy, as they would not integrate a check in SIS when checking their national security databases.

The use of API data for advanced compliance checks and targeting could allow EU stakeholders to maximise the benefits of API for their law enforcement and border management purposes, combining local and central checks and analyses with those performed today by national authorities. This leads to the maximised score for the effectiveness assessment of the border management and security objectives.

This would be the ultimate benefit of standardising and streamlining the collection and distribution of API - so that its processing could take place where it makes the most sense, in a way that is transparent to third-party stakeholders such as carriers. MCA: assessment of efficiency

The capital expenditure related to this scenario would include the following implications for border management and law enforcement authorities:

- Cost of setting up the interactive response, considering extra information coming from detected security patterns;
- Cost of setting up data analytics to detect risk patterns;
- Governance model with the Member States to define a common risk detection approach that could be used to centrally detect travellers' suspicious travel patterns.

As regards operating costs, staff in EU and national authorities might increase as a result of performing tasks for the ESP and CRRS[181]. However, there could also be savings in relation to staff costs, given the limited need to manage communication links with individual carriers. The redeployment of staff to new activities around the ESP and CRRS could mean that this scenario would be cost-neutral for border management and law enforcement authorities (in terms of staff costs).

Future centralised business applications that require API data to fulfil their business purposes would benefit from API data available via an interoperable system (CRM), significantly reducing development costs. From the perspective of efficiency benefit objective assessment, Scenario 4 enables the maximisation of API data by making it readily available to all local or central risks management application, an enabling these applications to report alerts directly back to the business operations (carriers, border management and law enforcement).

The additional costs would depend on the interoperability of the risk management applications that would use API data. As interoperability is a general requirement for new applications or evolutions of existing ones, low costs are expected for accessing API data in the context of scenario 4. As these applications are hypothetical at this stage, there is no basis for more detailed costs estimates.

Table 40. Overview of costs per stakeholder group

Stakeholder	**Estimated additional costs** ***Scenario 4***
Air Carriers	N/A
National Authorities	Low costs (receiving new alerts)
eu-LISA	Low costs extensions to CRM to interface with additional interoperable risk detection systems.

Source: ICF estimates

3.8.5.2 MCA: assessment of coherence

Apart from other instruments referred to in previous scenarios, the exchange of data as defined in the Interoperability Regulation would be streamlined. Regulation 2017/458 on the reinforcement of checks against relevant databases at external borders (for EU citizens and third-country nationals) should be mentioned, as it is expected that the systematic checks required under this Regulation (checks against SIS II, SLTD and national databases) would be facilitated as part of the central check.

[181] Central repository for reporting and statistics (CRRS)

3.8.5.3 MCA: assessment of fundamental rights

This scenario represents a significant change in the processing of data. There is no longer a change in the way data are being forwarded, but, rather, on how data are analysed and how decisions on travellers are made. The assessment of fundamental rights on centralised compliance checking and risk/targeting is, however, beyond the scope of this study.

Table 41. Overview of the assessment for policy option V, scenario 4

Policy option V, scenario 4			**Score**
Effectiveness	***General objectives***	Improve the management and protection of EU external borders	🟦🟦🟦🟦🟦
		Enhance the security of citizens in the EU	🟦🟦🟦🟦🟦
	Specific objectives	Improve border checks	🟦🟦🟦🟦🟦
		Facilitate flow of legitimate travellers at the EU external borders	🟦🟦🟦🟦🟦
		Combat irregular migration	🟦🟦🟦🟦🟦
		Contribute to the fight against serious crime and terrorism	🟦🟦🟦🟦🟦
	Auxiliary objective	Public health control	🟦🟦🟦□□
Overall effectiveness assessment			🟦🟦🟦🟦🟦
Efficiency	***Costs***	Carriers	N/A
		Border management authorities	🟧□□□□
		Law enforcement authorities	🟧□□□□
		eu-LISA	🟧□□□□
	Benefits	Better passenger data	🟦🟦🟦🟦🟦
		Better risk analysis	🟦🟦🟦🟦🟦
		Better operational planning	🟦🟦🟦🟦🟦
		Better operational response	🟦🟦🟦🟦🟦
Overall efficiency assessment			🟦🟦🟦🟦□
Coherence		Streamline API with international standards	🟦🟦🟦🟦□
		Objectives of the Schengen Borders Code	⬛⬛⬛□□
		Objectives of EES Regulation	⬛⬛⬛□□
		Objectives of ETIAS Regulation	⬛⬛⬛□□
		Objectives of VIS Regulation (and proposed recast)	⬛⬛⬛□□
		Objectives of the Interoperability Regulation	🟦🟦🟦🟦🟦
		PNR Directive objectives	⬛⬛⬛□□
Overall coherence assessment			🟦🟦🟦🟦□
Overall data protection and fundamental rights assessment			N/A

Legend

⬛ Scenario/assessment similar to the baseline (Scenario 0)

🟦 Scenario/assessment more favourable in comparison to the baseline (Scenario 0)

🟧 Scenario/assessment less favourable in comparison to the baseline (Scenario 0)

Annexes

Annex 1 List of abbreviations

A4E	Airlines for Europe
API	Advance Passenger Information
ARINC	Aeronautical radio incorporated
BCP	Border Crossing Point
BG	Border Guard
BMA	Border Management Authority
CG	Carrier Gateway
COM	European Commission
CRM	Central Routing Mechanism
CRS	Computerised Reservation Systems
CRRS	Central repository for reporting and statistics
CSCA	Country Signing Certification Authority
CUSRES	Customs Response Message
DCS	Departure Control System
DG HOME	Directorate-General for Migration and Home Affairs
DPIA	Data Protection Impact Assessment
EBCGA	European Border and Coast Guard Agency
EC	European Commission
ECDC	European Centre for Disease Prevention and Control
EDPS	European Data Protection Supervisor
EES	Entry/Exit-System
EIS	Europol Information System
ERAA	European Regions Airline Association
ESP	European Search Portal
EST	Electronic Travel System
ESTA	Electronic System for Travel Authorization (US)
ETIAS	European Travel Information and Authorisation System
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice
FRA	European Fundamental Rights Agency
GDPR	General Data Protection Regulation
i-API	interactive Advance Passenger Information
IATA	International Air Transport Association
IAM	Identity Access Management
IBM	Integrated Border Management
ICAO	International Civil Aviation Organization

ID	Identity
INAD	Inadmissible Passenger
IT	Information Technology
KOM	Kick Off Meeting
LEA	Law Enforcement Authorities
LED	Law Enforcement Directive
MRZ	Machine Readable Zone
MS	Member States
NAs	National Authorities
NBTC	National Border Targeting Centre
NGO	Non-Governmental Organization
NS	National System
OCR	Optical Character Recognition
OSCE	Organization for Security and Cooperation in Europe
PAXLST	Passenger List
PIU	Passenger Information Unit
PNR	Passenger Name Record
RFID	Radio Frequency Identification
RIU	Research and Innovation Unit
SAC	Schengen Associated Country
SIS	Schengen Information System
SITA	Société Internationale de Télécommunications Aéronautiques
SLA	Service Level Agreement
SLTD	Stolen and Lost Travel Documents Database
SW	Single Window
TCs	Third countries
TCNs	Third Country Nationals
UN	United Nations
VIS	Visa Information System
WCO	World Customs Organization
WHO	World Health Organization

Countries Abbreviations

AT	Austria
BE	Belgium
BG	Bulgaria
CH	Switzerland
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
ISL	Iceland
IT	Italy
LI	Liechtenstein
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	Netherlands
NO	Norway
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SI	Slovenia
SK	Slovak Republic

Annex 2 Glossary of terms

Advance Passenger Information (API) – Information concerning the passengers' identity, usually taken from their official documents as well as flight information for passengers, whom carriers will transport to an authorised border crossing point through which these persons will enter the territory of a Member State, which carriers are obliged to transmit, by end of check-in, at the request of responsible authorities carrying out checks on persons at external borders.[182]

API batch system – An electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival and made available on the primary line at the airport of entry.[183]

Border control – The activity carried out at a border, in accordance with and for the purposes of Regulation (EU) 2016/399 (Schengen Borders Code)[184], in response exclusively to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance.[185]

Border Crossing point – Any crossing point authorised by the competent authorities for the crossing of external EU borders.[186]

Carrier – A natural or legal person who provides passenger transport services by air.[187]

Carrier gateway (CG) – Web service enabled system, to be introduced in accordance with Regulation 2018/1240 establishing European Travel Information and Authorisation System (ETIAS)[188], allowing carriers to verify the authorisation status of third-country national (TCN) travellers.[189]

Charter flight/ Non-scheduled revenue flights (excluding on-demand flights)– Charter flights and special flights performed for remuneration other than those reported under scheduled flights. They *includ*e any items related to blocked-off charters and *exclude* air taxi, commercial business aviation or other on-demand revenue flights.[190]

Centralised Routing Mechanism – central point to which air carriers may submit passengers and crew manifests and which can forward the passengers data to other information systems (See single window).

Conformity checks – Checks carried out by carriers at the boarding gate to ensure that the passengers' names on boarding passes correspond to the name on their travel document.

[182] EMN Glossary: advance passenger information (API) https://ec.europa.eu/home-affairs/content/advance-passenger-information-api_en

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

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

[185] EMN Glossary: Border control https://ec.europa.eu/home-affairs/content/border-control-0_en

[186] EMN Glossary: Border crossing point https://ec.europa.eu/home-affairs/content/border-crossing-point-0_en

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

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

[189] Annex 8, Terms of Reference

[190] ICAO Glossary, https://www.icao.int/dataplus_archive/documents/glossary.docx

Entry / Exit System (EES) – A system which registers entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Schengen States.[191]

EU Advance Passenger Information (API) Directive 2004/82/EC[192] **-** The Directive requires carriers to communicate information on passengers travelling from a third country to a Member State to the responsible authority in charge of border checks at the external border at the time of passenger check-in. It aims at improving border controls and combating irregular migration. The Directive also permits Member States to use API data for law enforcement purposes under certain conditions.[193]

EU Passenger Name Record (PNR) Directive 2016/681 – The Directive provides for the transfer by air carriers of PNR data of passengers of extra-EU flights to the Member States and their processing and exchange by the Member States for the purposes of fighting terrorism and serious crime. Member States may notify the Commission that they intend to apply the Directive also to intra-EU flights. The Directive was adopted by the Parliament and the Council on 27 April 2016 and Member States were required to transpose it into national law by 25 May 2018.[194]

European Travel Information and Authorisation System (ETIAS) established by Regulation 2018/1240– An automated online system for identifying irregular migration, security or public-health risks associated with visa-exempt third-country nationals travelling to the EU prior to their arrival.[195]

External borders – The parts of a Schengen Member State's border, including land borders, river and lake borders, sea borders and their airports, river ports, seaports and lake ports, that are not common borders with another Schengen Member State.[196]

Extra-EU flight – Any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a EU Member State or flying from the territory of a EU Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries.[197]

Extra-Schengen flight - Any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the Schengen area territory or flying from the territory of the Schengen area and planned to land in a third country, including in both cases flights with any stop-overs in the territory of the Schengen area or third countries.

Extra-EU/Schengen flights – This term has been used in the Study for any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on an EU Member State or the Schengen area territory (i.e. the 32 States applying the API Directive) or flying from the territory of an EU Member State or the Schengen area and planned to land in a third country, including in both cases flights with any stop-overs in the territory of an EU Member States or the Schengen area or third countries.

[191] EMN Glossary: Entry/Exit System (EES) https://ec.europa.eu/home-affairs/content/entryexit-system-ees-0_en

[192] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0082

[193] API Directive https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082&from=EN

[194] Directive (EU) 2016/681 of the European Parliament and of the Council (PNR Directive) https://eur-lex.europa.eu/eli/dir/2016/681/oj.

[195] EMN Glossary: European Travel Information and Authorisation System (ETIAS) https://ec.europa.eu/home-affairs/content/european-travel-information-and-authorisation-system-etias_en.

[196] Article 2 of Regulation 2016/399 (hereafter the ‚Schengen Borders Code') https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0399

[197] Article 3 PNR Directive https://eur-lex.europa.eu/eli/dir/2016/681/oj.

Integrated border management (IBM) – National and international coordination and cooperation among all relevant authorities and agencies involved in border security to establish effective, efficient and coordinated border management at the external EU borders, in order to ensure secure borders.[198]

Interactive API System (i-API) – An electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities, who within existing business processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member.[199]

Interoperability – The ability of information systems to exchange data and enable sharing of information. In the context of border and migration management, it means that authorised users have faster, seamless and more systematic access to the information they need.[200]

Intra-EU flight – Any scheduled or non-scheduled flight by an air carrier flying from the territory of an EU Member State planned to land on the territory of one or more of the Member States, without any stop-overs in the territory of a third country.[201]

Intra-Schengen flight - Any scheduled or non-scheduled flight by an air carrier flying from one airport within the area without controls at internal borders (known as the Schengen Area[202]) planned to land at another airport within the Schengen area, without any stop-overs outside that area.

Intra-EU/Schengen flights – This term has been used in the Study for any scheduled or non-scheduled flight by an air carrier flying from the territory of an EU Member State or the Schengen area territory (i.e. the 32 States applying the API Directive) planned to land on the territory of one or more of the 32 Member States applying the Directive, without any stop-overs in the territory of a third country.

Irregular Migration – Movement of persons to a new place of residence or transit that takes place outside the regulatory norms of the sending, transit and receiving Member States.[203]

Measures – For the purpose of this study, measures represent plans or courses of action taken to achieve an effective processing of API data with clear rules and transparency, and in full consistency with the interoperability of EU information systems for borders, security and migration management purposes, EU data protection requirements, and other existing EU instruments and international standards, while ensuring facilitation of legitimate travellers.

Member States – In the context of this study, 'Member States' mean all the 31 States applying the API Directive -i.e. 27 Member States of the European Union and the Schengen associated countries (SACs) (i.e. Liechtenstein, Iceland, Norway, and Switzerland).

Options – For the purpose of this study, options represent course of actions to be taken in 6 policy areas, containing possible measures and underpinning scenarios. Options include a baseline situation and scenarios.

[198] EMN Glossary: European integrated border management https://ec.europa.eu/home-affairs/content/european-integrated-border-management_en.

[199] Annex 8, Terms of Reference.

[200] European Commission, Factsheet http://europa.eu/rapid/press-release_MEMO-17-5241_en.pdf.

[201] Article 3 PNR Directive https://eur-lex.europa.eu/eli/dir/2016/681/oj.

[202] The Schengen area encompasses 22 EU Member States, all except for Bulgaria, Croatia, Cyprus, Ireland, Romania. Four third countries, Iceland, Norway, Switzerland and Liechtenstein have joined the Schengen Area (Schengen associated countries – SAC): https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en

[203] EMN glossary: Irregular migration https://ec.europa.eu/home-affairs/content/irregular-migration-0_en.

Passenger – Any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person's registration in the passengers list.[204]

Passenger Information Unit (PIU) – Units established or designated within the law enforcement authorities dealing with terrorist offences and serious crime at Member State level that collect, store and process PNR data. They collect PNR data from air carriers, compare it against relevant law enforcement databases and process them against pre-determined criteria, in order to identify persons that may be involved in a terrorist offence or serious crime. They are also responsible for disseminating PNR data and the result of processing them to the national competent authorities, Europol and the PIUs of other Member States. [205]

Passenger Name Record (PNR) – 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 journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities.[206] PNR data can include API data if these were collected by the carrier for their commercial purposes.

Personal data – any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[207]

Processing of personal data – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[208]

Pull method – Method of data transmission whereby the competent authorities of the Member State requiring the PNR data can access the air carrier's reservation system and extract (‘pull’) a copy of the required PNR data.

Push method – Method of data transmission whereby, for example, data are transmitted by the carrier to the national authority instead of the national authority accessing the air carrier's reservation system and taking the data (pull method).[209]

Reservation system – The air carrier’s internal system, in which PNR data are collected for the handling of reservations.[210]

Roll-out/Pilot – In the context of policy or practices, a test implementation of a programme, system or operational practice to assess whether it should be introduced more widely.

Scenarios – For the purpose of this study, scenarios represent possible actions or events to be undertaken in the future for each measure in the 5 policy options.

[204] Article 3, PNR Directive, https://eur-lex.europa.eu/eli/dir/2016/681/oj.

[205] Article 4, PNR Directive, *Ibid.*

[206] Article 3, PNR Directive, *Ibid.*

[207] Article 4, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[208] Article 4, GDPR, *Ibid.*

[209] DG Home Glossary: Push method https://ec.europa.eu/home-affairs/content/push-method_en.

[210] Article 3, PNR Directive.

Schengen Information System (SIS) – An information system set up at EU level that enables the relevant authorities in each EU Member State and Schengen Associated Country, by means of an automated search procedure, to have access to alerts on persons and objects for the purposes of border checks and other police, customs and immigration checks.[211]

Serious crime – Offences listed in Annex II of the PNR Directive, punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.[212]

Single Window – A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfil all regulatory requirements. If information is electronic then individual data elements should only be submitted once.[213]

Stolen and Lost Travel Documents database (SLTD) – Database maintained by Interpol containing around 84 million records of lost, stolen and revoked travel documents, such as passports, identity cards, visas and UN laissez-passer, as well as stolen blank travel documents. Law enforcement officers at National Central Bureaus and at airports and border crossings around the world can check the validity of a travel document in seconds using the database.[214]

Third Country Nationals – Any person who is not a citizen of the European Union within the meaning of Article 20(1) of TFEU and who is not a person enjoying the right of free movement under Union law, as defined in Article 2(5) of Regulation (EU) 2016/399 (Schengen Borders Code).[215]

Visa Information System (VIS) – in accordance with Regulation 767/2008[216], system for the exchange of visa data between Schengen States, which enables authorised national authorities to enter and update visa data and to consult these data electronically.[217]

[211] EMN Glossary: Schengen Information System(SIS) https://ec.europa.eu/home-affairs/content/schengen-information-system-sis_en.

[212] Annex 2, PNR Directive.

[213] ICAO https://www.icao.int/Meetings/FALP/Documents/FALP9-2016/FALP9_WP9_Single-Window-Concept_IATA.pdf.

[214] Interpol https://www.interpol.int/en/How-we-work/Databases/Stolen-and-Lost-Travel-Documents-database

[215] EMN Glossary: Third-country national https://ec.europa.eu/home-affairs/content/third-country-national_en

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

[217] DG Home Glossary: Visa Information System (VIS) https://ec.europa.eu/home-affairs/content/visa-information-system-vis_en.

Annex 3 List of sources

Legal instruments

- Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 ('Carriers' liability') Link
- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (API Directive) Link
- 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 Link
- Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units Link
- Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data Link
- Interoperability 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 Link
- Regulation (EU) 2016/399 of the European Parliament and of the Council on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) Link
- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes Link
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) Link
- Commission Implementing Decision (EU) 2018/1547 of 15 October 2018 laying down the specifications for the connection of the central access points to the Entry/Exit System (EES) and for a technical solution to facilitate the collection of data by Member States for the purpose of generating statistics on the access to the EES data for law enforcement purposes Link
- Regulation (EU) 2017/458 if the European Parliament and of the Council of 15 March 2017 regarding the reinforcement of checks against relevant databases at external borders Link
- Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) Link
- Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Link
- Regulation 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU Link
- Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community Link

- Directive (EU) 2017/2109 of the European Parliament and of the Council of 15 November 2017 amending Council Directive 98/41/EC on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community and Directive 2010/65/EU of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States Link
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) Link
- Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) Link
- 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 and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA Link
- United Nations Security Council Resolution 2178/2014 on threats to international peace and security caused by Foreign Terrorist Fighters Link
- United Nations Security Council Resolution 2309/2016 on terrorist threats to civil aviation Link
- United Nations Security Council Resolution 2396(2017) on threats to international peace and security caused by terrorist acts Link
- United Nations Security Council Resolution 2482 (2019) on threats to international peace and security caused by international terrorism and organized crime Link

Policy documents

- European Commission, Staff Working Document, Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), SWD(2020)175, link
- European Commission, Communication on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime of 24 July 2020 COM (2020) 305 final
- European Commission, Communication to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, 2015 Link
- European Parliament, Substitute impact assessment Study. The European Commission package of ETIAS consequential amendments, 2019 Link
- European Commission, Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82, Final Report, September 2012 Link
- European Commission, Evaluation Study on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 – Final Report, March 2020 Link
- Feedback on the Roadmap for the Evaluation of the API Directive 2004/82/EC, 2018 Link
- European Commission, Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information and Passenger Name Records, 2019 Link
- G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism, 26-27 May 2017 Link

- European Commission, Impact Assessment accompanying Proposal establishing a framework for interoperability between EU information systems (borders and visa), 2017 Link
- European Commission, Impact Assessment accompanying Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime Link
- OSCE Ministerial Council Decision 6/16 of December 2016 Enhancing the use of Advance Passenger Information Link
- European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data A Toolkit, 2017 Link
- European Data Protection Supervisor, Proportionality Guidelines aimed at making privacy-friendly policymaking easier Link
- European Commission, Report on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 2020 Link
- European Commission, Technical Study on Smart Borders. Final Report. DG HOME, 2014 Link
- European Commission, Evaluation of the Systematic Checks Regulation (not yet published)
- European Commission, Impact Assessment Report on the establishment of an EU Entry Exit System, 2016 Link
- European Commission, Feasibility Study for a European Travel Information and Authorisation System (ETIAS), 2016 Link
- European Commission, Study on the feasibility and implications of options to digitalise visa processing, 2010 Link
- European Commission, Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents, 2018 Link
- eu-LISA, Entry/Exit System (EES) Working Group on ICT Solutions for External Borders (sea/land) Report, 2019 Link
- Frontex, Report on API systems and targeting centres, 2018 (not published)

International and EU level sources

- Convention on International Civil Aviation (Chicago Convention), Annex 9 (Facilitation), 2017 Link
- Convention on Facilitation of International Maritime Traffic, 1965
- Council of Europe (2015), Passenger Name Records, data mining and data protection
- A4E, IATA Feedback on the Roadmap for the Evaluation of the API Directive 2004/82/EC
- European Commission, Technical Study on Smart Borders, Final Report 2014
- Frontex Report on API Systems and Targeting Centres
- FRA Fundamental rights at airports: Border checks at five international airports in the European Union, 2014
- ICAO Doc. 9303 on Machine-Readable Travel Documents Link
- ICAO The Implementation Steps of Advance Passenger (API) System
- ICAO Working paper on the Harmonisation of Advance Passenger Information (API) Regimes
- ICAO Working paper on the Harmonisation of Advance Passenger Information Requirements
- ICAO/WCO/IATA Management Summary on Passenger-related Information Link
- Interpol, Stolen and Lost Travel Documents database

- OSCE, Overview of Advance Passenger Information (API) in the OSCE Area, 2017 Link
- Report from the United Nations Counter-Terrorism Executive Directorate on Gaps in the use of advance passenger information and recommendations for expanding its use to stem the flow of foreign terrorist fighters Link
- FRA, Under watchful eyes: Biometrics, EU IT systems and fundamental rights, 2018
- WCO/IATA/ICAO Guidelines on Advance Passenger Information (API) Link
- IATA Vision 2050 Report
- World Economic Forum, The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel, 2018, Link

Other reports and sources

- Council of Europe, Passenger Name Records, data mining & data protection: the need for strong safeguards, 2015 Link
- ICAO, Harmonisation of Advance Passenger Information (API) Regimes, 2018 Link
- OSCE, Overview of the use of Advance Passenger Information (API) in the OSCE Area, 2018 Link
- ICAO, The Implementation Steps of Advance Passenger (API) System, 2018 Link
- OECD, ITF, Discussion Paper on Toward Risk-Based Aviation Security Policy, 2008 Link
- ICAO, Traveller Identification Programme (TRIP) Revised Implementation Roadmap for Member States, 2019 Link
- ICAO, ICAO, TRIP Guide on Evidence of identity, 2018 Link
- TRIP Strategy Compodium, A key overview of the traveller identification management, 2017 Link

Opinions

- European Data Protection Supervisor, On the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record Data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 2011 Link
- Article 29 Data Protection Working Party, Recommendation 1/98 on Airline Computerised Reservation Systems (CRS), 28 April 1998, WP 10 Link
- Article 29 Data Protection Working Party, Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, 19 January 2005, WP 103 Link
- Article 29 Data Protection Working Party, Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data, 27 September 2006, WP 127 Link
- FRA Opinion 1/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (Article 29 Data Protection Working Party) Link
- FRA Opinion 2/2018, The revised Visa Information System and its fundamental rights implications (2018) Link

Case law

- Court of Justice of the European Union (CJEU), Opinion 1/15 of 26 July 2017 on the draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data Link

- CJEU, joined cases Touring Tours & Travel, C-412/17, C-472/17 Link

Academic sources and statistical sources

- API and PNR data in use for border control authorities (source: surveys)
- Rossi dal Pozzo, F., EU Legal Framework for Safeguarding Air Passenger Rights. Link
- eu-LISA, SIS II 2018 Statistics Link
- Eurostat 2017/2018 growth in total passenger air transport by Member State Link
- Eurostat, Energy, transport and environment statistics — 2019 edition Link
- Eurostat, Maritime ports freight and passenger statistics, Increase in seaborne goods and passengers in EU ports, 2018 Link
- Eurostat, Passenger Transport Statistics, 2018, Link
- IATA Air Traffic Statistics Link
- Statista Number of scheduled passengers boarded by the global airline industry from 2004 to 2021
- Kaunert, C., Leonard, S. and Mackenzie, A., The European parliament in the external dimension of EU counter-terrorism: More actorness, accountability and oversight 10 years on? Intelligence and National Security, 2015 Link
- Liu, Y., James, H., Gupta, O. and Raviv, D., MRZ code extraction from visa and passport documents using convolutional neural networks, 2020, Link
- Pozzo, F., EU Legal Framework for Safeguarding Air Passenger Rights. 2015
- E. Zureik and M. Salter,What happens when you book an airline ticket? The collection and processing of passenger data post-911. Global Surveillance and Policing: Borders, Security, Identity 2005 Link
- Han, C., McGauran, R. & Nelen, H., API and PNR data in use for border control authorities, 2017 Link

Annex 4 Extension of the collection of PNR data to other modes of transport

While the scope and subject of the Study is the assessment of the potential effects of different possible measures on API, this annex provides a succinct overview of extending PNR to other modes of transport (policy option III). The information below is based on desk research and data collected from the stakeholder consultations.

Contextual background to the PNR Directive

The API Directive regulates the collection of API data for border control purposes and allows the collection and transfer of API data for law enforcement purposes on the basis of national law.

Adopted in 2016, Directive 2016/681 on the use of Passenger Name Record (PNR Directive)[218] provides a legal basis for Member States to collect API data from air carriers if those API data elements have been already collected in the carriers' systems. Accordingly, Annex I to the PNR Directive includes API data among the data to be sent by carriers if air carriers have collected such data in the normal course of their business. However, whereas the primary objective of the API Directive is border control and preventing irregular migration, the objective of the PNR Directive is law enforcement. The API Directive also foresees the use of API data for law enforcement purposes when the use of such data is authorised by national law in line with the enabling clause in Article 6(1) last sub-paragraph. API data help Member States to verify the identity of an individual, increasing the added value of (unverified) PNR data. The collection and processing of API data is regulated at EU level by two different legal instruments (i.e. API and PNR Directives) for different purposes. This has led to some inconsistencies in the application of the two Directives at national level (e.g. the data retention period). In practice, 29 Member States collect API data for border control purposes and 21 Member States for law enforcement purposes[219].

Member States are required to establish PIUs, which are responsible for the PNR database. PIUs compare PNR data against relevant law enforcement databases and process those data against predetermined criteria in order to identify people that may be involved in terrorist offences or serious crime.

Broadening PNR Directive's scope to other modes of transport

Similar to the API Directive, Article 1 of the PNR Directive specifies the scope to include 'air carriers' only. In some Member States, PNR data are already collected from forms of transport other than air traffic. According to the 2020 European Commission's Report on the implementation of PNR, Belgium extends the collection of PNR data to international high-speed trains and the international bus sector, although that implementation is at a very early stage. Estonia collects ferry passengers' data. French legislation foresees the collection of API and PNR for maritime transport. In Sweden, the police and customs authority have access to passengers' data from other modes of transport, but the scope of the applicable legislation is more limited than the PNR Directive[220]. These regulations are still in their early implementation and have yet to be evaluated.

In practice, the data collected by Member States from other modes of transport covers biographical information from travellers (similar to API data) rather than actual booking information, which is generally limited in mode of transports other than air. There is no

[218] 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, OJ L 119, 4.5.2016.

[219] completed in 2020. evaluation.

[220] Commission Staff Working Document, SWD(2020) 128 final.

PNR standard in maritime or land transport industries (unlike air transport). Each carrier shares, on an ad hoc basis, the information they might collect in their booking systems, such as:

- Seating information (coach, seat for trains, cabin for cruise);
- Travelling party (how many people in the same booking);
- Vehicle information for ferries;
- Payment methods;
- Any contact information (primarily phone numbers);
- Any information on travel agencies.

In 2019, members of the Informal Working Group on Passenger Name Record (IWG PNR) were surveyed on their views on broadening the scope of the PNR Directive to other types of transportation[221]. The majority of the Member States agreed on broadening the scope of the PNR Directive: 83% wanted to broaden it to maritime, 76% to railway, and 67% to road traffic. Those not in favour highlighted that the increase of data to be processed by the PIU was unlikely to be manageable and could even be seen as interfering with the right to privacy. Overall, Member States were in favour of broadening the scope of data collection to other types of transportation, but suggested that it was important to first implement the PNR Directive in order to ensure that PIUs are fully operational and can manage the PNR data.

In the context of increased maritime passenger traffic, the Finnish Presidency suggested continuing the discussion about widening the scope of the PNR Directive to other forms of transportation than air traffic, specifically pointing to 'sea traffic and international high-speed trains'[222].

In November 2019, the Council Conclusions on widening the scope of the use of PNR data to forms of transport other than air traffic were adopted[223]. The Council acknowledged that traffic volumes both within and outside the Schengen area are increasing. Alongside air traffic, ferries, ships, boats, trains and buses carry large numbers of passengers across the borders on a daily basis.

The Council also highlighted that gathering and analysing PNR data and closely related API data is important for combating terrorism and serious crime: '*Through handling and analysing PNR and API data, law enforcement authorities' actions and resources are directed in a more efficient and targeted way*.'

Some Member States welcomed the initiative and acknowledged the potential added value for preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Others, however, voiced concerns about the timing and likely legal, technical and financial challenges, notably with regard to fundamental rights and the principles of proportionality and necessity. The Council recommended that the European Commission conduct '*a thorough impact assessment on widening the scope of the PNR Directive to cross-border forms of transport other than air traffic*.'

According to the Report on the review of PNR Directive, although the collection of PNR data from other transport modes could contribute to closing a security gap, it would also raise practical, technical and legal questions, including on fundamental rights. Each transportation mode is discussed briefly below.

[221] Working Party on the Information Exchange and Data Protection (DAPIX), available at: https://www.statewatch.org/media/documents/news/2019/jul/eu-council-pnr-policy-debate-6300-19.pdf

[222] Available at: https://data.consilium.europa.eu/doc/document/ST-11433-2019-INIT/en/pdf https://data.consilium.europa.eu/doc/document/ST-11433-2019-INIT/en/pdf

[223] https://data.consilium.europa.eu/doc/document/ST-14061-2019-INIT/en/pdf

Rail carriers

In 2019, in response to Council discussions, the Community of European Railways (CER) submitted a position paper on the widening of scope to rail carriers[224]. CER presented a number of arguments against the expansion of scope of PNR to rail carriers. Similar to the arguments to the expansion of scope of the API Directive, CER pointed to the lack of infrastructure and reservation systems, lack of nominative tickets, and the business model (turn-up-and-go) and booking processes.

Infrastructure difficulties in implementing PNR data collection and transmission are due to their inherent differences with air transport: i.e. open infrastructure, intermediate stops where passengers can embark or disembark, sharing of platforms among different types of trains, high numbers of passenger stations, etc.

This was confirmed by the data collected for this Study, which found that few rail carriers have reservation systems that systematically collect passenger data – even those that do hold data of much lower quality than air carriers.

According to CER, the vast majority of rail operators do not have a system in place to collect and transmit traveller/passenger data to national authorities. Eurostar is due to launch a PNR data-sharing pilot with Belgium. After scoping discussions with UK and Belgian authorities, the launch faced delays due to the COVID-19 pandemic and UK-EU Brexit negotiations. It is now planned for the second half of 2021.

The UK border authorities already collect API data from Eurostar travellers on outbound routes. This is part of the UK's Exit Programme. As the UK does not have exit border checks, carriers are requested to send a complete list of passport information from passengers leaving the UK. In the case of Eurostar, Mitie (Eurostar's security provider in UK terminals) collects travel document (passport and national ID card) details of passengers exiting the UK at the UK-EU border after check-in, before boarding. However, the data are collected on behalf of UK border force based on the UK Immigration Act 1971, with Eurostar acting as a data processor on its behalf. Eurostar has no visibility of this information other than at an anonymised aggregate level.

Maritime carriers

The PNR Directive does not include maritime carriers in its scope. There are several types of maritime carriers (including sea and river carriers) for different purposes, including passenger transport. According to the IMO, while there are no universally applicable definitions of ship types, specific descriptions and names are used within IMO treaties and conventions. A passenger ship is defined as a ship that carries more than 12 passengers[225].

The WCO is in the process of setting up a working group for the establishment of a global standard for API/PNR data standard for cruise ships and a related compendium, as a precursor for other transport sectors[226]. The API and PNR global standards will be established for cruise ships and then extended to ferries and (possibly) other maritime areas[227].

Several Member States, such as Estonia and France, collect (or plan to collect) PNR and API for maritime transport. Estonia collects ferry passengers' data and French legislation foresees the collection of API and PNR for maritime transport.

Some Member States' border management and law enforcement authorities interviewed Member States (e.g. Finland) noted a significant increase in both maritime traffic and passengers in recent years. Those Member States in favour of expanding the scope of

[224] https://www.cer.be/sites/default/files/publication/191108_CER_PositionPaper_PNR.pdf

[225] SOLAS - International Convention for the Safety of Life at Sea I/2.

[226] http://www.wcoomd.org/en/media/newsroom/2020/october/14th-session-of-the-wco-iata-icao-api-pnr-contact-committee.aspx

[227] Interview with the WCO, an international organisation.

the API and PNR Directives to maritime stated that a lot of maritime carriers are coming from countries considered at risk of migration flows or even terrorism. In terms of the benefits, one Member State noted that connecting every transport modality to the PIU in terms of API data transmission would have advantages in eliminating gaps in the movement of suspects, describing the modus operandi in full detail, querying watchlists and databases and in better detecting, investigating and preventing crimes[228]. Another emphasised that the quality of API data in combination with PNR is expected to be higher, as the data requirements for API are not as good as those for PNR[229]. They further underlined that the best approach for law enforcement authorities would be to use and store API data in the same way as PNR data.

Overland coaches

Currently, there are no international standards for the collection of passenger data for coach operators. According to industry representatives, there are a number of sector-specific limitations in relation to physical and digital infrastructure. The digitalisation of the road transport sector has remained somewhat limited and collection of passenger data is not a specific focus for coach operators, thus there are limited online reservation systems.

According to the industry representatives consulted, there is very limited collection of API data through reservation systems of coach and bus carriers. Imposing an obligation on carriers to collect and transmit passenger data would require investment in IT systems. The decentralisation of the sector, however, would make it prohibitive for small and medium-sized companies to invest in such IT systems. The possible solutions and their cost-effectiveness (mobile app, NFC reader) could be considered (see policy option IV).

Unfortunately, no coach operators participated in the Study (a number of refusals were received from coach operators) and the practice has not been confirmed with coach operators. Interviews with industry representatives (IRU) confirmed that journey forms are routinely collected and some operators may collect very limited personal data of passengers for safety and security reasons.

The coach transport sector in Europe is decentralised, with many small and medium sized companies[230], many with small fleets (3-100 coaches). Data on the number of extra-EU cross-border journeys by coach are not readily available. COVID-19 saw a significant decrease in the number of connections, thus they cannot be extrapolated from current timetables.

[228] Interview with Romanian PIU, national authority.

[229] Interview with Finnish PIU, national authority.

[230] Industry estimates 3,000-5,000 coach companies in the EU.

Annex 5 Multicriteria analysis

As per Toolbox #63 of the Better Regulation Guidelines, Multi-Criteria Analysis (MCA) method can help to establish preferences between a sub-set of scenarios by reference to an explicit set of objectives and measurable criteria. MCA offers a possibility to aggregate complex set of evidence (including monetary, quantitative, and qualitative information) against individual criteria to provide an assessment of the overall performance of different options/scenarios.

The first step of the MCA is to define and elaborate the criteria for the assessment and to set the respective scoring or weighting. Following the Terms of Reference and the key aspects for assessment indicated, the main criteria for assessing the options and possible measures for a revision of the API Directive are fourfold:

- Effectiveness,
- Efficiency,
- Coherence,
- Respect of personal data protection and of the fundamental rights of data subjects.

Table 39 below outlines the key elements which form part of the assessment as well as a pre-assigned individual and overall weight. The MCA takes an artificially constructed approach whereby weighting is pre-assigned to each criterion. Given the importance of all the four criteria, we suggest assigning equal weights of 25% to each criterion. Each criterion is then composed of a number of components and each component is assigned individual weight.

Table 42. Proposed weightings for Multi-criteria analysis

Criteria	#	Impact	Means of assessment	Individual weight	Overall weight
Effectiveness	1	To what extent would the scenario achieve the desired objectives (in terms of general, specific and operational objectives) for **border control purposes**?	Qualitative assessment Likert scale 0 to 5 score (*0 = no change compared to the status quo; 5 = maximum contribution to the objectives*)	15%	**25%**
	2	To what extent would the scenario achieve the desired objectives (in terms of general, specific and operational objectives) for **law enforcement purposes**?		10%	
Efficiency (CBA)	3	Would the scenario result in additional direct costs?	Monetisation of costs incurred by different stakeholder types Assessment of who would bear the costs	4%	**25%**
	4	Would the scenario result in additional administrative burden?	Monetisation of costs Assessment of who would bear the burden or indirect costs	3%	
	5	What are the technological implications of the scenario?	Qualitative assessment Complexity and costs of the scenario	3%	
	6	What are the operational implications of the scenario?	Qualitative assessment Complexity and costs of the scenario	3%	
	7	What are the organisational implications of the scenario?	Qualitative assessment Complexity and costs of the scenario	3%	

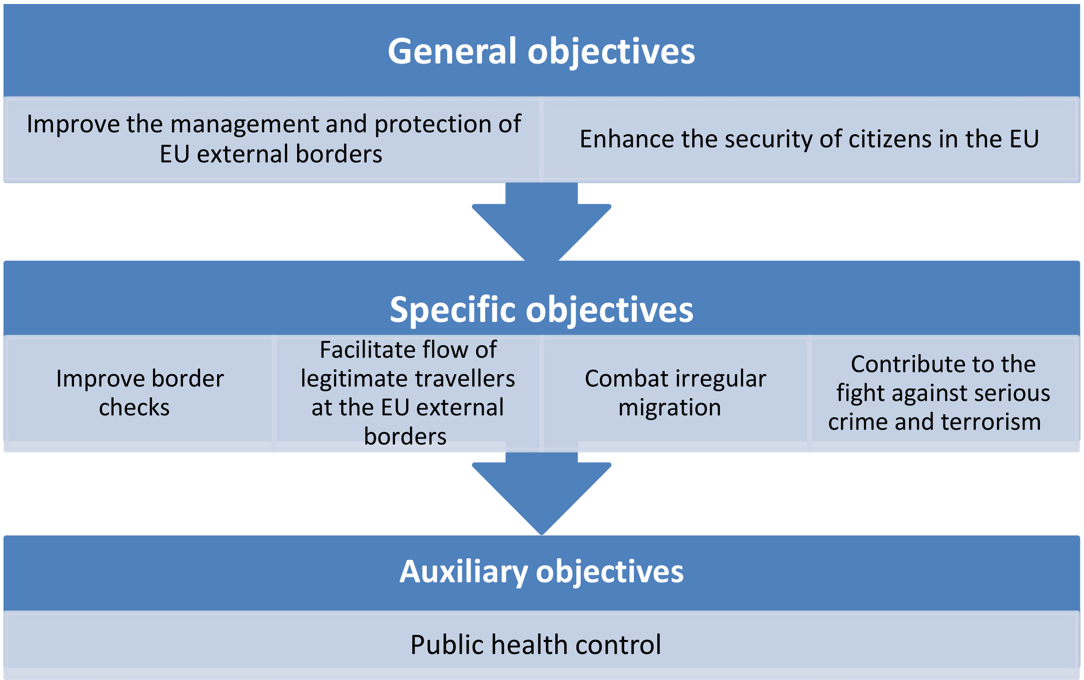
	8	Is this scenario likely to increase or decrease the demand for passenger transport per passenger mode of transport?	Qualitative assessment and if possible projections	3%	
	9	What are the benefits of the scenario (e.g. minimisation of security gaps)?	Cost-benefit ratios	10%	
Coherence	10	To what extent the option further clarifies and streamlines the legislative framework?	Qualitative assessment Likert scale 0 to 5 score	10%	**25%**
	11	To what extent is the option coherent with ETIAS/EES(VIS) Regulations? PNR Directive?	Qualitative assessment Likert scale 0 to 5 score	15%	
Compliance with data protection	12	To what extent does the scenario comply with the necessity principle of the processing operations?	Qualitative assessment Likert scale 0 to 5 score	6.25%	**25%**
	13	To what extent does the scenario comply with the proportionality principle of the processing operations?	Qualitative assessment Likert scale 0 to 5 score	6.25%	
	14	To what extent does the scenario present risks to the personal data protection principles?	Qualitative assessment Likert scale 0 to 5 score	6.25%	
	15	To what extent does the scenario identify potential mitigating measures to address the risks?	Qualitative assessment Likert scale 0 to 5 score	6.25%	

Criteria 1: Effectiveness

Effectiveness assesses the extent to which the possible measures or options can realistically achieve the objectives stated for the intervention.

The stated objectives for a revision of the API Directive are suggested as per below:

Figure 14. Hierarchy of objectives of API


General objectives
Improve the management and protection of EU external borders
Enhance the security of citizens in the EU
Specific objectives
Improve border checks
Facilitate flow of legitimate travellers at the EU external borders
Combat irregular migration
Contribute to the fight against serious crime and terrorism
Auxiliary objectives
Public health control

The assessment will be compiled in the form of the following table using a Likert scale (0 = no change compared to the status quo; 5 = maximum contribution to the objectives).

The rationale for the scoring under each objective is developed in a qualitative manner. Naturally, the assessment of the contribution towards the general objective will reflect the anticipated impact of the scenarios. The contribution towards the specific objectives will reflect the anticipating results or outcomes of the scenarios, and the contribution towards the operational objectives will reflect the anticipated operational benefits of each of the scenarios. Such rationale will be based on the triangulation of the evidence gathered through surveys, interviews and expert opinions. The distinction between border control and management purposes and law enforcement perspective will be made in an accompanying narrative (note that each types of objective relate to one or the other purpose).

Criteria 2: Efficiency

Efficiency assesses the extent to which the possible measures generate benefits which outweigh the costs. The assessment is hence split into two parts:

- *Costs:* The calculations of the cost implications of the different measures will be provided by the cost model (see Annex 6).
- *Operational benefits:* They can be described according to four main benefit areas:
  - Better passenger data (higher quality, enhanced access / availability, increased breadth and of the data reported (volume and scope);
  - Better risk analysis (improved situational awareness / intelligence picture);

- Better operational planning capability (ability to plan and conduct border checks / law enforcement activities);
- Better operational response (speed, and cost of response).

The assessment of the operational benefits for each scenario will build on the pro-forma (i.e. the performance indicators) sent to Member States, surveys, interviews and expert opinions.

The assessment will be compiled in the form of the following table using a Likert scale for the assessment of benefits (0 = no change compared to the status quo; 5 = maximum benefits generated). The rationale for the scoring under each benefit area will be developed in a qualitative manner summarising the evidence gathered through the variety of sources aforementioned. The distinction between border control and management purposes and law enforcement perspective will be made in an accompanying narrative to the table.

The overall cost / benefit ratio will be summarised drawing on the two separate assessments (e.g. high costs / high benefits). A supporting rationale for the overall score will be provided in a narrative form.

Criteria 3: Coherence

Coherence assesses the complementarity of each option with the objectives of relevant EU policies. The relevant EU policies in the field identified at interim stage are:

- ETIAS and EES Regulations (and recast VIS Regulation at the moment of writing the report)
- PNR Directive
- Regulation on Interoperability between EU information systems in the field of justice, freedom and security
- Other instruments as appropriate (e.g. Schengen Border Code, SIS)

The assessment of the coherence each of the scenario with other EU policies in the field will build on desk research, interviews, surveys and expert opinion. The assessment will be compiled in the form of the following table using a Likert scale for the assessment of coherence (0= objective contradicting one another; 5 = fully aligned objectives). The rationale for the scoring under each benefit area will be developed in a qualitative manner summarising the evidence gathered through the variety of sources aforementioned. The distinction between border control and management purposes and law enforcement perspective will be made in an accompanying narrative to the table.

The overall coherence score will be elaborated drawing on the separate coherence scores against each of the relevant policies under consideration. A supporting rationale for the overall score will be provided in a narrative form.

Criteria 4: Data protection and fundamental rights principles

This criterion asses, for each policy option extending the scope of the use of API data, their impact on data protection and fundamental rights. API data are personal data, the processing of which should respect the fundamental rights of protection of private life and personal data protection as recognised by Articles 7 and 8 of the Charter on Fundamental Rights of the European Union, as well as Article 16 of the Treaty on the Functioning of the European Union. These rights can be however subject to limitations and conditions defined in the Charter and permit interferences in so far as necessary.[231] Any interference with personal data must be necessary and proportionate. These two principles stand at the core of the assessment in this task,[232] which also aims to identify

[231] Article 52(1) EU Charter of Fundamental Rights.

[232] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf; EDPS, Assessing the necessity of measures that limit the

possible operational and technical safeguards to enable the lawful collection and use of API data, thus increasing the legal certainty for both national authorities and passengers (data subjects).

The assessment will be compiled in the form of the following table using a Likert scale summarising the DPIA for specific areas. The rationale for the scoring under each benefit area will be developed in a qualitative manner summarising the evidence of the DPIA (e.g. safeguards, security measures or mechanism ensuring the respect of the data protection principles and or fundamental rights). The overall score will be elaborated drawing on the separate assessments. A supporting rationale for the overall score will be provided in a narrative form.

fundamental right to the protection of personal data: A Toolkit, 2017, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

Annex 6 Approach to estimating costs

This note provides a detailed description of the methodological approach undertaken to estimate costs associated with: (i) existing API data requirements; and (ii) new, additional requirements entailed by several (future) policy options foreseen by the Commission.

This section is structured as follows:

- Section 1 discusses general assumptions underlying the estimation of costs;
- Section 2 describes the approach taken to estimate baseline or existing costs arising from compliance with current API data requirements;
- Section 3 describes the approach taken to estimate additional costs likely to arise from the implementation of Policy Option 1;
- Section 4 describes the approach taken to estimate additional costs likely to arise from the implementation of Policy Option 2;
- Section 5 describes the approach taken to estimate additional costs likely to arise from the implementation of Policy Option 3;
- Section 6 describes the approach taken to estimate additional costs likely to arise from the implementation of Policy Option 4; and,
- Section 7 describes the approach taken to estimate additional costs likely to arise from the implementation of Policy Option 5.

A6.1 General assumptions

key assumptions were made to support the estimation/ quantification exercise.

A6.1.1 Types of costs

The costs entailed by current and new API data requirements comprise both:

- **One-off costs**, i.e. costs that will be paid only once at the time of the investment; and,
- **Recurring costs**, i.e. costs that will be paid at regular intervals. Such costs are typically required for operating a business/ an organisation .

One-off costs and recurring costs can be 'fixed' or 'variable' in nature. Fixed costs are those costs, paid once or at regular intervals, that remain constant over time. Variable costs, on the other hand, are proportional to the scope and volume of activity. For instance, in the context of this study, variable costs would typically vary in accordance with the volume of API data, the volume of passengers, etc..

The main cost categories considered are presented in the table below. Cost implications will differ in accordance with the policy option being considered. Selected / relevant cost categories will be discussed for each policy option in subsequent sub-sections.

Main cost categories

Cost category	Sub cost category	Type of cost
One-off costs, i.e. fixed or variable costs paid only once		
Building / infrastructure	Acquisition / upgrade / re-design of border infrastructure or public key infrastructure	Fixed
	Acquisition / upgrade of building security	
Connectivity /API data exchange capacity	Acquisition / upgrade of communication infrastructure (e.g. link(s) to carriers, EU-LISA carrier gateways, routing of API data flows, link(s) to national watch-list and EU databases, etc.)	Fixed
Equipment costs	Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers	Fixed
	Acquisition / upgrade of IT business applications / software to process / check API data	Fixed
	Acquisition / upgrade of IT equipment (i.e. hardware) receive API data from EU-LISA (carrier gateway)	Fixed
	Redesign of standard operating procedures (for data collection, data access, data processing, data triage and forwarding)	Fixed
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Operational staff costs	Costs associated with new / additional management staff	Variable
	Costs associated with new / additional IT technical support staff (infrastructure / equipment)	
	Costs associated with new / additional technical support staff (business applications / software)	
	Costs associated with new / additional API data quality controllers (e.g. for reporting and solving data quality issues)	
	Costs associated with new / additional API data analysts (e.g. for processing and dispatching API data)	
Other staff costs	Staff training costs	Variable
Ongoing communication / connectivity costs	Costs of connectivity with carriers / EU LISA	Fixed / or variable
	Other data exchange fees	
Recurring IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	Fixed

	Costs associated with regular maintenance of business / data applications
	Costs associated with regular maintenance of communication infrastructure

A6.1.2 Affected groups

Having to comply with existing and new API data requirements will bring about direct costs for:

- **transport operators**, comprising air carriers, maritime transport operators, rail transport operators, and bus/coach services; and,
- **national authorities**, i.e. border management authorities (BMAs) and law enforcement authorities (LEAs).

Indirect costs (e.g. impact on prices for passengers) have not been quantified, though they are discussed qualitatively.

A6.1.3 Data gaps

It is assumed that Member States with relatively similar passenger flows incur or will incur similar cost levels. This assumption helps address data gaps as it allows for cost estimation or extrapolation among ‘clusters’ of Member States. The ‘clusters’ have been decided based on the (total) number of passengers (arriving/departing by air, sea, rail and land) experienced by Member States. Data on passengers were sourced from Eurostat.

The following ‘clusters’ were identified.

Clusters	Member States concerned
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovenia, Slovakia, Iceland, Liechtenstein
Cohort 2	Austria, Belgium, Czech Republic, Denmark, Finland, Greece, Ireland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland
Cohort 3	Germany, France, Italy, Spain

A6.2 Estimating the 'baseline'

Note: the calculation of the baseline cost is for illustrative purposes only. It has no bearing on the calculation of costs associated with each individual option.

A6.2.1 Direct costs to BMAS and LEAs

A6.2.1.1 Acquisition / upgrade of building security

Data on costs associated with the acquisition/ upgrade of building security have been provided by authorities in **Belgium** and **Iceland** only. No further data on costs were available. The following values have therefore been used to estimate costs for other Member States.

Minimum value	Average value	Maximum value	Source(s)
EUR 300,000	EUR 650,000	EUR 1,000,000	Data gathered from survey with BMAs/LEAs

Note: minimum and maximum values based on Belgium's estimates; average value calculated as: (300,000+1,000,000/2)= EUR 650,000

It is assumed that the minimum value is at least incurred by Member States within Cohort 1, i.e. those with the lowest passenger flows; the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3. Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovenia, Slovakia, Iceland, Liechtenstein	EUR 300,000
Cohort 2	Austria, Belgium, Czech Republic, Denmark, Finland, Greece, Ireland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland	EUR 650,000
Cohort 3	Germany, France, Italy, Spain	EUR 1,000,000

A6.2.1.2 Acquisition / upgrade of communication infrastructure (e.g. link(s) to carriers, EU-LISA carrier gateways, routing of API data flows, link(s) to national watch-list and EU databases, etc.)

Data on costs associated with the acquisition / upgrade of communication infrastructure have been provided by authorities in **Belgium**, **France** and **Malta** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Minimum value	Average value	Maximum value	Source(s)
EUR 39,000 (rounded)	EUR 72,000 (rounded)	EUR 104,000 (rounded)	Data gathered from survey with BMAs/LEAs

Note: minimum value based on France's estimates and maximum value on Malta's estimates; average value calculated as: (39,000+104,000/2)= EUR 43,000. Note: we feel estimates provided by the Belgian authorities are too high (min value: EUR 500,000; max value: EUR 800,000) and do not propose using them for extrapolation purposes.

It is assumed that the minimum value is incurred by Member States within Cohort 1 (as handling lower passenger levels most likely requires fewer investments); the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3 (who most likely spend the most owing to much larger passenger flows they handle). However, these estimates are only used where cost data are not available for Member States.

Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovenia, Slovakia, Iceland, Liechtenstein	EUR 39,000
Cohort 2	Austria, Czech Republic, Denmark, Finland, Greece, Ireland, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Switzerland	EUR 72,000
	Belgium	EUR 675,000[233]
	Malta	EUR 104,000
	Sweden	EUR 62,000 (rounded)[234]
Cohort 3	Germany, Italy, Spain	EUR 104,000
	France	60,000 (rounded)[235]

A6.2.1.3 Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers

Data on costs associated with the acquisition / upgrade of IT equipment to collect data from carriers have been provided by authorities in **Belgium**, **Malta** and **Slovenia** respectively. We also have data from ICF's past evaluation (dated 2019). The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

[233] Data provided by Belgian authorities. Estimate has been calculated as the average of minimum and maximum values provided: (550,000+800,000/2)= EUR 675,000

[234] Data provided by Swedish authorities. Estimate has been calculated as the average of minimum and maximum values provided: (42,000+81,000/2)= EUR 62,000

[235] Data provided by French authorities. Estimate has been calculated as the average of minimum and maximum values provided: (30,000+89,000/2)= EUR 60,000

Minimum value	Maximum value	Average value	Source
Estimates gathered from various sources			
EUR 132,000*	EUR 2,000,000**	EUR 1,000,000 (rounded)	Data gathered from survey with BMAs/LEAs
EUR 300,000 (for a basic API system)	EUR 2,000,000 (for a fully advanced API system)	EUR 1,150,000	Data gathered from ICF's past evaluation
Final estimates proposed			
EUR 200,000 (rounded)[236]	**EUR 2,000,000[237]**	**EUR 1,100,000[238]**	**Calculated**

Note: [*]: minimum value based on Ireland's estimates; [**]: maximum value based on Malta's estimates

It is assumed that the minimum value is incurred by Member States within Cohort 1 (as handling lower passenger levels most likely requires fewer investments); the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3 (who most likely spend the most owing to much larger passenger flows they handle). However, these estimates are only used where cost data are not available for Member States.

Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovakia, Iceland, Liechtenstein	EUR 200,000
	Slovenia	EUR 110,000[239]
Cohort 2	Austria, Czech Republic, Finland, Greece, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Switzerland	EUR 1,100,000
	Belgium	EUR 1,050,000
	Denmark	EUR 340,000 (rounded)
	Ireland	135,000 (rounded)
	Malta	EUR 2,000,000
	Sweden	EUR 24,000
Cohort 3	Germany, France, Spain	EUR 2,000,000
	Italy	EUR 240,000

[236] Estimate has been calculated as: (132,000+300,000/2)= EUR 200,000 (rounded)

[237] Estimate has been calculated as: (1,800,000+2,000,000/2)= EUR 1,900,000

[238] Estimate has been calculated as: (200,000+1,900,000/2)= EUR 1,050,000

[239] Estimate has been calculated as the average of minimum and maximum values provided by Slovenian authorities: (13,000+206,000/2)= EUR 110,000

A6.2.1.4 Acquisition / upgrade of IT business applications / software to process / check API data

Data on costs associated with the acquisition / upgrade of IT applications/ software to process/ check API data have been provided by authorities in **Belgium**, **Italy**, **Malta**, **Iceland**, **Switzerland**, **Slovenia** and **Slovakia** respectively. We also have data from ICF's past evaluation (dated 2019). The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Minimum value	Maximum value	Average value	Source
Estimates gathered from various sources			
EUR 56,000*	EUR 1,800,000**	EUR 928,000	Data gathered from survey with BMAs/LEAs
EUR 9,000	EUR 750,000	EUR 379,500	Data gathered from ICF's past evaluation
Final estimates proposed			
EUR 33,000 (rounded)[240]	**EUR 1,300,000 (rounded)**[241]	**EUR 700,000 (rounded)**[242]	**Calculated**

Note: [*]: minimum value based on Switzerland's estimates; [**]: maximum value based on Belgium's estimates

It is assumed that the minimum value is incurred by Member States within Cohort 1 (as handling lower passenger levels most likely requires fewer investments); the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3 (who most likely spend the most owing to much larger passenger flows they handle). However, these estimates are only used where cost data are not available for Member States.

Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Romania Liechtenstein	EUR 33,000
	Luxembourg	EUR 20,000[243]
	Slovenia	EUR 50,000[244]
	Slovakia	EUR 250,000[245]
	Iceland	EUR 200,000[246]

[240] Estimate has been calculated as: (9,000+56,000/2)= EUR 33,000

[241] Estimate has been calculated as: (750,000+1,800,000/2)= EUR 1,300,000

[242] Estimate has been calculated as: (33,000+1,300,000/2)= EUR 700,000

[243] Estimate has been calculated as the average of values provided over the 2018-2020 period: (15,000+21,000+24,000+206,000/3)= EUR 20,000

[244] Estimate has been calculated as the average of minimum and maximum values provided by Slovenian authorities: (1,000+100,000/2)= EUR 50,000 (rounded)

[245] Estimate obtained from Slovakian authorities

[246] Estimate obtained from Icelandic authorities

Clusters	Member States concerned	Estimated costs
Cohort 2	Austria, Greece, Ireland, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal	EUR 700,000
	Belgium	EUR 1,100,000 (rounded)[247]
	Czech Republic	EUR 40,000 (rounded)[248]
	Denmark	EUR 900,000 (rounded)[249]
	Finland	EUR 29,000 (rounded)[250]
	Malta	EUR 900,000 (rounded)[251]
	Sweden	EUR 400,000 (rounded)[252]
	Switzerland	EUR 80,000 (rounded)[253]
Cohort 3	Germany, France, Spain	EUR 1,300,000
	Italy	EUR 6,000,000 (rounded)[254]

A6.2.1.5 Redesign of standard operating procedures (for data collection, data access, data processing, data triage and forwarding)

Data on costs associated with the redesign of standard operating procedures have been provided by authorities in **Finland** only. They provide an estimate of **EUR 70,000** (as of 2015)[255].

We therefore assume that Member States within Cohort 2 (which also comprises Finland) incur at least EUR 70,000 as a result of having to redesign standard operating procedures. To estimate costs for other Member States, we look at differences in passenger flows among the different cohorts. Eurostat data on the number of passengers indicate that, on average:

- Member States within Cohort 1 handle twice as less passengers as Member States within Cohort 2 (i.e. the ratio of passengers handled by Member States in Cohort 1 versus Cohort 2 is 1:2); and

[247] Estimate has been calculated as the average of minimum and maximum values provided by Belgian authorities: (400,000+1,800,000/2)= EUR 1,100,000

[248] Estimate obtained from Czech authorities

[249] Estimate has been calculated as the average of minimum and maximum values provided by Danish authorities: (800,000+1,000,000/2)= EUR 900,000

[250] Estimate has been calculated as the average of minimum and maximum values provided by Finnish authorities: (27,000+30,000/2)= EUR 29,000 (rounded)

[251] Estimate obtained from Maltese authorities

[252] Estimate has been calculated as the average of minimum and maximum values provided by Swedish authorities: (200,000+600,000/2)= EUR 400,000 (rounded)

[253] Estimate has been calculated as the average of minimum and maximum values provided by Swiss authorities: (60,000+104,000/2)= EUR 80,000 (rounded)

[254] Estimate obtained from Italian authorities

[255] Please note that there is no indication of whether these estimated costs constitute a minimum, maximum or an average value. We assume it is a maximum value

- Member States within Cohort 3 handle twice as many passengers as Member States within Cohort 2 (i.e. the ratio of passengers handled by Member States in Cohort 3 versus Cohort 2 is 2:1).

We apply these proportional differences or ratios to obtain cost estimates for all Member States within Cohort 1 and Cohort 3. Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia, Slovakia, Iceland, Romania Liechtenstein	EUR 35,000[256]
Cohort 2	Austria, Belgium, Czech Republic, Denmark, Greece, Finland, Ireland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland	EUR 70,000
Cohort 3	Germany, France, Italy, Spain	EUR 140,000[257]

A6.2.1.6 Costs associated with new / additional management staff

Data on costs associated with new/ additional management staff have been provided by authorities in **Ireland, the Netherlands and Iceland respectively**. The estimates provided below relate to average cost per worker/ staff member i.e. **yearly salary per staff member**.

Minimum value	Maximum value	Average value	Source
EUR 35,000*	EUR 113,000**	EUR 74,000	Data gathered from survey with BMAs/LEAs

Note: [*]: minimum value based on Ireland's estimates; [**]: maximum value based on the Netherlands' estimates

Based on the above data, we assume that average salary for one member of staff in management (across all Member States) is at least EUR 74,000 per year. We further assume that the number of staff members required rises with the volume of passengers experienced by Member States. Hence, the more passengers the higher the overall staff costs.

Data gathered from Ireland indicates that management staff may comprise a total of five people. As before, we use proportional differences in passenger flows (or ratios) across Member States to estimate the number of people employed at management level.

The estimates used for the calculation of costs associated with management staff are as follows.

[256] Estimate calculated as: (EUR 70,000/2) = EUR 35,000

[257] Estimate calculated as: (EUR 70,000*2) = EUR 140,000

Clusters	Member States concerned	Estimated annual salary	Estimated number of management staff
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia, Slovakia, Iceland, Romania Liechtenstein	EUR 74,000	3
Cohort 2	Austria, Czech Republic, Denmark, Greece, Finland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland	EUR 74,000	5
	Belgium	EUR 74,000	7[258]
	Ireland	EUR 35,000	5[259]
	Netherlands	EUR 100,000 (rounded)[260]	15
Cohort 3	Germany, France, Italy, Spain	EUR 74,000	10

A6.2.1.7 Costs associated with new / additional IT technical support staff (infrastructure / equipment)

Data on costs associated with new/ additional IT technical support staff (infrastructure/ equipment) have been provided by authorities in **Belgium**, **Denmark**, **Slovenia** and **Iceland respectively**. The estimates provided below relate to average cost per worker/ staff member i.e. **yearly salary per staff member**.

Minimum value	Maximum value	Average value	Source
EUR 15,000*	EUR 87,000**	EUR 51,000	Data gathered from survey with BMAs/LEAs

Note: [*]: minimum value based on Slovenia's estimates; [**]: maximum value based on Denmark's estimates. The above estimates are costs per worker/ FTE

Based on the above data, we assume that average salary for one member of staff in technical support (across all Member States) is at least EUR 51,000 per year. We further assume that the number of staff members required rises with the volume of passengers experienced by Member States. Hence, the more passengers the higher the overall staff costs.

The data/ evidence does not provide any indication of the number of technical support staff members required. It is therefore assumed that the technical support staff is at

[258] Data on total costs associated with management staff were provided by the Belgian authorities. These were estimated at: EUR 485,000. Assuming an average salary of EUR 74,000, it is assumed that at least 7 people are employed at management level

[259] Data on total costs associated with management staff (including number of staff at management level) were provided by the Irish authorities

[260] Data on total costs associated with management staff were provided by the Dutch authorities. These were estimated at about: EUR 1,700,000 (rounded). It was also indicated that about 15 people are employed (although it is not certain whether they all work in management). Based on this information, it is assumed that each worker earns about EUR 100,000 (rounded) per annum

least as big as the management team; hence, we use similar numbers (pertaining to staff) as before (see previous sub-section).

The estimates used for the calculation of costs associated with technical support staff are as follows.

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia, Slovakia, Iceland, Romania Liechtenstein	EUR 51,000	3
Cohort 2	Austria, Czech Republic, Denmark, Greece, Finland, Ireland, Latvia, Lithuania, Malta, Norway, Poland, Portugal, Sweden, Switzerland	EUR 51,000	5
	Belgium		7
	Netherlands		15
Cohort 3	Germany, France, Italy, Spain	EUR 51,000	10

A6.2.1.8 Costs associated with new / additional technical support staff (business applications / software)

Data on costs associated with new / additional technical support staff (business applications / software) have been provided by authorities in **Belgium** and **Denmark respectively**. The estimates provided below relate to average cost per worker/ staff member i.e. **yearly salary per staff member**.

Minimum value	Maximum value	Average value	Source
EUR 50,000	EUR 87,000	EUR 69,000	Data gathered from survey with BMAs/LEAs

Note: [*]: minimum and maximum values based on Denmark's estimates. The above estimates are costs per worker

Based on the above data, we assume that average salary for one member of staff in technical support (across all Member States) is at least EUR 69,000 per year. We further assume that the number of staff members required rises with the volume of passengers experienced by Member States. Hence, the more passengers the higher the overall staff costs.

Data/ evidence from Danish authorities indicate that about three members of staff are required in the technical support (business applications/ software) team. We use proportional differences in passenger flows (or ratios) across Member States to estimate the number of people employed at management level (i.e. Cohort 1: Cohort 2 = 1:2; and Cohort 3: Cohort 2= 2:1).

The estimates used for the calculation of costs associated with technical support staff are as follows.

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia, Slovakia, Iceland, Romania Liechtenstein	EUR 69,000	2
Cohort 2	Austria, Belgium, Czech Republic, Denmark, Greece, Finland, Ireland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland	EUR 69,000	3
Cohort 3	Germany, France, Italy, Spain	EUR 69,000	6

A6.2.1.9 Costs associated with new / additional API data quality controllers (e.g. for reporting and solving data quality issues)

Data on costs associated with new / additional API data quality controllers have been provided by authorities in **Belgium**, **Denmark** and **Iceland respectively**. The estimates obtained from the different authorities relate to total staff costs. No information has been provided on the number of workers or FTE the costs relate to.

Minimum value	Maximum value	Average value	Source
EUR 55,000	EUR 640,000	EUR 348,000	Data gathered from survey with BMAs/LEAs

Note: [*]: minimum value based on Iceland's estimates; [**]: maximum value based on Belgium's estimates

In the absence of data, we assume that the number of API data quality controllers required is at least on par with the number of people required at management level; hence three API data quality controllers for Member States within Cohort 1; five for Member States within Cohort 2; and 10 for Member States within Cohort 3.

The estimates used for the calculation of costs associated with the recruitment of API data quality controllers are thus as follows.

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia, Slovakia, Iceland, Romania Liechtenstein	EUR 74,000[261]	3
Cohort 2	Austria, Belgium, Czech Republic, Denmark, Greece, Finland, Ireland, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Sweden, Switzerland		5

[261] Calculated as average of: (348,000/3); (348,000/5); (348,000/10) = EUR 74,000 (rounded)

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
Cohort 3	Germany, France, Italy, Spain		10

A6.2.1.10 Costs associated with new / additional API data analysts (e.g. for processing and dispatching API data)

Data on costs associated with new / additional API data analysts have been provided by authorities in **Belgium**, **Italy** and **Iceland respectively**. The estimates obtained from the different authorities relate to total staff costs. No information has been provided on the number of workers or FTE the costs relate to.

We can assume that the number of API data analysts required will likely depend on the extent/ amount of API data that need to be processed/ analysed. Hence, the larger the amount of API data collected, the higher the number of data analysts who may be required. ICF's past evaluation[262] provides the following information on the share of passengers for whom API data are collected across some Member States.

Share of passengers (%) for whom API data are collected

CH	CZ	FI	HR	IE	LT	MT	NL
42%	88%	100%	7%	13%	29%	53%	100%

Source: ICF and Unisys (2019). Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data.'

In the absence of data, we assume that Member States with significant API data collection – 80 per cent or more – (i.e. most likely Member States within Cohort 3 and some Member States within Cohort 2) will require an additional 15 data analysts[263]; those with relatively important API data collection – 50 to 80 per cent – (i.e. most of the Member States within Cohort 2) will require an additional 10 data analysts[264]; and those with less important API data collection – up to 15 per cent – (i.e. most likely Member States within Cohort 1) will require about three additional analysts[265].

The estimates used for the calculation of costs associated with the recruitment of API data quality controllers are thus as follows.

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovenia,	EUR 22,000[266]	3

[262] ICF and Unisys. 2019. 'Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data.' Available at: file:///C:/Users/30205/Downloads/DR0420133ENN.en.pdf

[263] This assumption is based on known additional FTE recruited at management level by Dutch authorities, which is 15 additional managers. We assume that, for every manager, one additional analyst is recruited; hence 15 additional data analysts for Member States, which like the Netherlands, gather large amounts of API data

[264] We use simple proportions/ ratios here, i.e. for Member States gathering API data for between 50% and 80% of passengers, an additional: [average of (15/100*50) and (15/100*79)]=10 data analysts may be required

[265] We use simple proportions/ ratios here, i.e. for Member States gathering API data for up to 15% of passengers, an additional: [15/100*15]=3 data analysts may be required

[266] Based on total staff costs for Iceland and Italy. Average staff costs for Iceland (assuming 3 additional analysts) = (62,000/3) = EUR 21,000; average staff costs for Italy (assuming 15 additional analysts): (333,000/15) = EUR 22,200. Average annual salary for analyst across Member States: (21,000+22,200/2) = EUR 22,000

Clusters	Member States concerned	Estimated annual salary	Estimated number of staff
	Slovakia, Iceland, Romania Liechtenstein		
Cohort 2	Austria, Belgium, Denmark, Greece, Latvia, Norway, Poland, Portugal, Sweden,		10
	Czech Republic		15[267]
	Finland		15[268]
	Ireland		3[269]
	Lithuania		5[270]
	Malta		10 (rounded)[271]
	Netherlands		15[272]
	Switzerland		6[273]
Cohort 3	Germany, France, Italy, Spain		15

A6.2.1.11 Costs of connectivity with carriers / EU LISA

Data on ongoing costs associated with connectivity with carriers/ EU LISA have been provided by authorities in **Belgium**, **Italy**, **Sweden**, **Slovakia** and **Iceland** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Member States concerned	Minimum value	Maximum value	Average value	Source
Cohort 1 (Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovenia, Liechtenstein)[274]	EUR 24,000*	EUR 150,000**	EUR 87,000	Data gathered from survey with BMAs/LEAs

[267] ICF's past evaluation indicates that CZ gathers API data for 88% of passengers; it is therefore assumed that CZ will require the maximum number of (additional) analysts, i.e. 15 data analysts

[268] ICF's past evaluation indicates that FI gathers API data for 100% of passengers; it is therefore assumed that FI will require the maximum number of (additional) analysts, i.e. 15 data analysts

[269] We use simple proportions/ ratios here, i.e. [15/100*13]=3 data analysts

[270] We use simple proportions/ ratios here, i.e. [15/100*30]=5 data analysts

[271] We use simple proportions/ ratios here, i.e. [15/100*53]=10 data analysts (rounded)

[272] ICF's past evaluation indicates that NL gathers API data for 100% of passengers; it is therefore assumed that NL will require the maximum number of (additional) analysts, i.e. 15 data analysts

[273] We use simple proportions/ ratios here, i.e. [15/100*42]=6 data analysts

[274] For Slovakia, we will use the estimates provided by Slovak authorities, i.e. average value: EUR 24,000; for Iceland, we will use average value: EUR 150,000

Member States concerned	Minimum value	Maximum value	Average value	Source
Cohort 2 (Austria, Czech Republic, Denmark, Finland, Greece, Ireland Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Switzerland)[275]	EUR 33,000***	EUR 500,000*****	EUR 200,000 (rounded)	
Cohort 3 (Germany, France, Spain)[276]	EUR 66,000	EUR 1,000,000	EUR 500,000 (rounded)	
Italy	EUR 1,300,000	EUR 2,200,000	EUR 1,750,000	

Note: [*]: minimum value based on Slovakia's estimates; [**]: maximum value based on Iceland's estimates . [***]: minimum value based on Sweden's estimates; [****]: maximum value based on Belgium's estimates

A6.2.1.12 Other data exchange fees

Data on ongoing costs associated with other data exchange fees have been provided by authorities in **Belgium**, **Luxembourg** and **Iceland** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Minimum value	Maximum value	Average value	Source
EUR 23,000*	EUR 100,000**	EUR 62,000	Data gathered from survey with BMAs/LEAs

Note: [*]: minimum value based on Switzerland's estimates; [**]: maximum value based on Belgium's estimates

It is assumed that the minimum value is at least incurred by Member States within Cohort 1, i.e. those with the lowest passenger flows (hence lowest API data transmissions); the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3. Cost estimates used across the 'clusters' are therefore as follows.

Clusters	Member States concerned	Estimated costs
Cohort 1	Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Romania, Slovenia, Slovakia, Liechtenstein	EUR 23,000
	Iceland	EUR 26,000[277]
Cohort 2	Austria, Czech Republic, Denmark, Finland, Greece, Ireland, Latvia, Lithuania, Malta,	EUR 62,000

[275] For Sweden, we will use the estimates provided by Swedish authorities, i.e. average value: EUR 33,000; for Belgium, we will use average value: (250,000+500,000/2) = EUR 375,000

[276] Estimates for Member States within Cohort 3 are calculated on the basis of the ratio of passengers between Member States in Cohort 3 to Member States in Cohort 2, i.e. 2:1. Minimum value is therefore calculated as: (33,000*2) = EUR 66,000 and maximum value: (500,000*2) = EUR 1,000,000. Values provided by Italy are not used for Member States within Cohort 3 as the estimates appear too high

[277] Provided by Icelandic authorities

Clusters	Member States concerned	Estimated costs
	Netherlands, Norway, Poland, Portugal, Sweden	
	Belgium	EUR 100,000[278]
	Switzerland	EUR 23,000[279]
Cohort 3	Germany, France, Italy, Spain	EUR 100,000

[278] Provided by Belgian authorities

[279] Provided by Swiss authorities

A6.2.1.13 Costs associated with regular maintenance of IT equipment and other related infrastructure

Data on ongoing costs associated with regular maintenance of IT equipment/ other related infrastructure have been provided by authorities in **Belgium**, **Denmark**, **Ireland**, **Slovenia**, **Switzerland**, and **Iceland** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Member States concerned	Minimum value	Maximum value	Average value	Source
Cohort 1 (Bulgaria, Croatia, Cyprus, Estonia, Hungary, Luxembourg, Slovakia, Romania, Slovenia, Liechtenstein)[280]	EUR 10,000*	EUR 30,000**	EUR `20,000	Data gathered from survey with BMAs/LEAs
Cohort 2 (Austria, Czech Republic, Finland, Greece, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal)[281]	EUR 50,000***	EUR 300,000****	EUR 175,000 (rounded)	
Cohort 3 (Germany, France, Italy, Spain)[282]	EUR 100,000	EUR 600,000	EUR 350,000	Estimated

Note: [*]: minimum value based on Iceland's estimates; [**]: maximum value based on Slovenia's estimates; [***]: minimum value based on Sweden's estimates; [****]: maximum value based on Denmark' s estimates (Belgium's estimate of EUR 800,000 is considered an outlier value (being too high) and is therefore not used as maximum value for Cohort 2)

A6.2.1.14 Costs associated with regular maintenance of business / data applications

Data on ongoing costs associated with regular maintenance of IT equipment/ other related infrastructure have been provided by authorities in **Belgium**, **Finland**, **Switzerland** and **Iceland** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Member States concerned	Minimum value	Maximum value	Average value	Source
Cohort 1 (Bulgaria, Croatia, Cyprus, Estonia, Hungary, Iceland Luxembourg, Slovakia, Slovenia, Romania, Slovenia, Liechtenstein)	n/a	n/a	EUR 32,000*	Data gathered from survey with BMAs/LEAs

[280] For Iceland, we will use the estimates provided by Icelandic authorities, i.e. average value: EUR 10,000; for Slovenia, we will use average value: EUR 30,000

[281] For Belgium, we will use the estimates provided by Belgian authorities, i.e. EUR 800,000; for Sweden, average value: EUR 50,000; for Denmark, average value: EUR 335,000; for Ireland: EUR 139,000; for Switzerland, EUR 80,000 (rounded)

[282] Estimates for Member States within Cohort 3 are calculated on the basis of the ratio of passengers between Member States in Cohort 3 to Member States in Cohort 2, i.e. 2:1. Minimum value is therefore calculated as: (50,000*2) = EUR 100,000 and maximum value: (300,000*2) = EUR 600,000.

Member States concerned	Minimum value	Maximum value	Average value	Source
Cohort 2 (Austria, Czech Republic, Denmark, Greece, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal)[283]	EUR 32,000**	EUR 170,000***	EUR 100,000	
Cohort 3 (Germany, France, Italy, Spain)[284]	EUR 64,000	EUR 340,000	EUR 200,000	Estimated

Note: [*]: estimate based on Sweden's estimated minimum value; [**]: minimum value based on Sweden's estimates; [***]: maximum value based on Switzerland's estimates (Belgium's estimate of EUR 600,000 is considered an outlier value (being too high) and is therefore not used as maximum value for Cohort 2)

A6.2.1.15 Costs associated with regular maintenance of communication infrastructure

Data on ongoing costs associated with regular maintenance of IT equipment/ other related infrastructure have been provided by authorities in **Belgium**, **Finland**, **Switzerland** and **Iceland** respectively. The following values have therefore been retained to estimate costs for Member States, where cost data are not available.

Minimum value	Maximum value	Average value	Source
EUR 3,000*	EUR 100,000**	EUR 52,000 (rounded)*	Data gathered from survey with BMAs/LEAs

Note: [*]: estimate based on Iceland's estimates; [**]: minimum value based on Belgium's budget for maintenance of communication infrastructure, i.e. EUR 500,000/5 = EUR 100,000

It is assumed that the minimum value is at least incurred by Member States within Cohort 1; the average value by Member States within Cohort 2; and the maximum value by Member States within Cohort 3.

A6.2.2 Direct costs to carriers

Estimates of costs for carriers are lacking, though a few sources, including: (1) cost data newly-gathered from consultations (carried out as part of this research); (2) cost data available from secondary sources (e.g. past evaluations) provide some indication of costs. The estimates gathered are as follows.

Cost data available from multiple sources

Source	Cost item	Estimate
ICF consultation (present research)	Additional management staff	EUR 50,000/ year (source: Luxair)
	Flat-rate contracts with external service providers (e.g. Amadeus, SITA)	EUR 50,000/ year (source: Luxair)

[283] For Belgium, we will use the estimates provided by Belgian authorities, i.e. EUR 600,000; for Sweden, average value: EUR 64,000; for Switzerland, average value: EUR 130,000 (rounded)

[284] Estimates for Member States within Cohort 3 are calculated on the basis of the ratio of passengers between Member States in Cohort 3 to Member States in Cohort 2, i.e. 2:1. Minimum value is therefore calculated as: (32,000*2) = EUR 64,000 and maximum value: (170,000*2) = EUR 340,000.

Source	Cost item	Estimate
	General/ overall set-up costs (API)	EUR 200,000 – EUR 500,000
2019 evaluation	General/ overall set-up costs (API)	Up to EUR 500,000

IATA explained that costs to (air) carriers can vary significantly. As such, "*for a low-cost domestic carrier with a basic in-house system, the development of a more advanced/ full-fledged API system could take less time and cost less; whereas for a network carrier with tens of different systems producing and using the data on 100+ locations it could take months to deploy, thus such a system would be more costly*."

We use the estimates provided by Luxair and IATA and extrapolate the data to obtain estimates for Member States where no data have been provided. Before calculating the costs:

- we select the main airline, i.e. the airline with the most passengers; and
- we classify each airline/ Member State into the following categories:
  - Cohort 1 ("small") – i.e. Member States with airlines serving less than 50 locations/ destinations;
  - Cohort 2 ("medium") – i.e. Member States with airlines serving between 51 and 100 locations/ destinations;
  - Cohort 3 ("large") – i.e. Member States with airlines serving more than 100 locations/ destinations.

In line with IATA's remarks, we assume that airlines serving a wider network of passengers/ destinations will require a more complex, thereby a more costly, API system than airlines serving fewer destinations. The cohorts of Member States are set out in 0 below.

The following cost values have been estimated for the different cohorts.

Cost estimates across the different cost categories

Cost item	Average value	Member States concerned
High-level costs		
Cost of sending one batch API	n/a	n/a
Cost of sending API data for one passenger	n/a	n/a
Cost of sending reservation data	n/a	n/a
Cost of sending reservation data for one passenger	n/a	n/a
Annual cost of flat rates contracts your carriers have	EUR 50,000[285]	Cohort 1
	EUR 100,000[286]	Cohort 2

[285] This is based on the estimate provided by Luxair, which is part of Cohort 1. We therefore assume that carriers operating in Member States within Cohort 1 incur at least EUR 50,000

[286] This is based on estimated proportional differences. IATA estimates that the overall costs associated with the implementation of an API system ranges between EUR 200,000 (for smaller airlines) and EUR 500,000 (for larger airlines.). We therefore assume costs of about: (EUR 200,000 + EUR 500,000/2) = EUR 350,000 for medium-sized airlines. This means that medium-sized airlines (operating in Member States in Cohort 2) would be incurring twice (i.e. EUR 350,000/EUR 200,000) the costs incurred by small-sized airlines (operating in Member States in Cohort 1) and large-sized airlines (operating in Member States in Cohort 3) would be incurring two and a half times more than small-sized airlines (operating in Member States in Cohort 1).

Cost item	Average value	Member States concerned
with external service providers	EUR 125,000	Cohort 3
One-off costs		
Building/ infrastructure		
Acquisition / upgrade / re-design of passenger flow management infrastructure	n/a	n/a
Acquisition / upgrade of data exchange infrastructure capabilities	n/a	n/a
Connectivity /API data exchange capacity		
Acquisition / upgrade of data exchange connectivity capabilities	n/a	n/a
Equipment		
Acquisition / upgrade of IT equipment (i.e. hardware)	n/a	n/a
Acquisition / upgrade of Departure Control System (DCS)	n/a	n/a
Acquisition / upgrade of computer reservation systems (CRS)	EUR 275,000[287]	Luxembourg
Acquisition / upgrade of biometric ID system	n/a	n/a
Acquisition of automatic capture tools of information contained in travel document	n/a	n/a
Investment in technology and operations for capturing new data not found in travel document	n/a	n/a
Investment in new business processes for collecting and processing API data	n/a	n/a
Integration of Departure control systems with other systems	n/a	n/a
Note: overall set-up costs estimated to range between EUR 200,000 (small airlines) and EUR 500,000 (large airlines) by IATA. These estimates are retained; for medium airlines, overall set-up costs are calculated as: average(200,000, 500,000) = EUR 350,000		
Recurring costs		
Operational staff costs		
	EUR 50,000[288]	Cohort 1

[287] Estimate provided by Luxair

[288] Estimate provided by Luxair; so it is assumed that all other airlines operating in Member States in Cohort 1 incur at least EUR 50,000 in management staff costs; and based on proportional differences, (50,000*2) for airlines operating in Member States in Cohort 2; and (50,000*2.5) for airlines operating in Member States in Cohort 3

Cost item	Average value	Member States concerned
Costs associated with new / additional management staff	EUR 100,000	Cohort 2
	EUR 125,000	Cohort 3
Costs associated with new / additional technical support agent	n/a	n/a
Costs associated with new / additional API data quality	n/a	n/a
Costs associated with new / additional check in or boarding gate agents	n/a	n/a
Costs associated with new / additional check in or boarding gate agents	n/a	n/a
Other staff costs		
Staff training costs	n/a	n/a
Ongoing communication / connectivity costs		
Cost of sending 1 API message (batch)	n/a	n/a
	n/a	n/a
	n/a	n/a
Cost of sending 1 API per passenger	n/a	n/a
Cost of “flat rates contracts with service providers	n/a	n/a
Other costs (rental costs of systems, Software as a service costs, etc.)	n/a	n/a
Ongoing IT infrastructure costs (maintenance and IT support)		
Costs associated with regular maintenance of IT equipment and other related infrastructure	n/a	n/a
Costs associated with regular maintenance of business systems / data applications	n/a	n/a
Costs associated with regular maintenance of communication infrastructure	n/a	n/a

Cohorts of Member States

Member State	Main airline(s)	Number of passengers	Number of destinations served	Cohort (assigned)
Austria	**Austrian Airlines**	14.0 million (as of 2018)	Flag carrier. Serves over 130 destinations predominantly in Europe, and some routes to USA and Asia	Cohort 3
	Lauda Air	2 million (as of 2019)	Low-fare airlines. Operates leisure flights	

Member State	Main airline(s)	Number of passengers	Number of destinations served	Cohort (assigned)
			and charters to holiday destinations in Europe, North Africa, the Caribbean and South-East Asia.	
	flyNiki	n/a	A scheduled semi-low cost airline; operates charter services to leisure destinations in Europe and Egypt	
Belgium	**Brussels Airlines**	10 million (as of 2019)	Main airlines in Belgium. Operates flights to more than 40 European destinations as well as flights to 16 destinations on the African continent	Cohort 2
Bulgaria	**Bulgaria Air**	n/a	Flag carrier. Operates regular flights from Sofia to: 29 major cities in Europe and the Middle East; regular domestic flights to Varna and Bourgas; charter flights by request to more than 100 destinations	Cohort 1
Croatia	**Croatia Airlines**	2 million (as of 2017)	National flag carrier of the Republic of Croatia. Serves the Balkan region and destinations in Europe	Cohort 1
Cyprus	**Cyprus Airways**	400,000 (as of 2019)	Operates scheduled services to 21 destinations in Europe and the Middle East	Cohort 1
Czech Republic	**Czech Airlines**	3 million (as of 2017)	Operates scheduled services to 69 destinations in 41 countries in Europe, the Middle East, North Africa and Asia.	Cohort 2
Denmark	**Scandinavian Airlines System (SAS)**	30 million (as of 2017)	Flag carrier of Denmark, Norway and Sweden. The airline operates flights to 176 destinations in more than 30 countries	Cohort 3
Estonia	**Estonian Air**	500,000	National airline, operates flights to destinations in north- and central Europe and western Russia	Cohort 1
Finland	**Finnair**	15 million (as of 2019)	Flag carrier and largest airline of the country. The airline connects Finland with 10	Cohort 2

Member State	Main airline(s)	Number of passengers	Number of destinations served	Cohort (assigned)
			destinations in Asia and over 50 cities in Europe.	
France	**Air France**	104 million (as of 20190	French flag carrier. The airline operates worldwide scheduled passenger and cargo services to 150 destinations in 90 countries as well as more than 30 destinations in France	Cohort 3
Germany	TUI fly	12 million (as of 2019)	Operates charter and scheduled low-cost flights predominantly to classic holiday regions around the Mediterranean, the Canary and Cape Verde Islands, Madeira and Egypt, as well as to cities in Europe, Africa, USA, and Asia	Cohort 3
	Lufthansa	145 million (as of 2019)	Flag carrier of Germany; largest airline in Europe. Operates services to 18 German cities and to more than 180 international destinations world-wide.	
Greece	**Aegean Airlines**	15 million (as of 2019)	Largest Greek airline; operates mainly domestic scheduled and charter services from Athens and Thessaloniki. Flies to 153 destinations	Cohort 3
Hungary	**Wizz Air**	40 million (as of 2019)	Ultra-low-cost airline; serves many cities across Europe, as well as some destinations in North Africa and the Middle East. Flies to 150 destinations	Cohort 3
Ireland	Aer Lingus	12 million (as of 2019)	National carrier; operates flights to destinations in Europe, North America and northern Africa	Cohort 3
	Ryanair	152 million (as of 2019)	Europe's largest low-cost airline; connects over 240 destinations in 40 countries	
Italy	**Alitalia**	23 million (as of 2019)	Flag airline; serves over 100 destinations	Cohort 3
Latvia	**AirBaltic**	4 million (as of 2018)	Flag carrier	Cohort 1
Lithuania	n/a	n/a	n/a	Cohort 1

Member State	Main airline(s)	Number of passengers	Number of destinations served	Cohort (assigned)
Luxembourg	**Luxair**	2 million (as of 2019)	Flag carrier airline; operates scheduled services to 50 destinations in Europe, North Africa, the Mediterranean and Middle East, as well as charter and seasonal services	Cohort 1
Malta	**Air Malta**	2 million (as of 2018)	National airline; operates services to more than 36 destinations in Europe and North Africa	Cohort 1
Netherlands	**KLM**	35 million (as of 2019)	National airline; operates scheduled passenger and cargo services to about 145 destinations worldwide	Cohort 3
Poland	**Polish Airlines**	10 million (as of 2019)	National airline; serves 60 destinations in Europe, the Middle East, North America, and Asia	Cohort 2
Portugal	**Air Portugal**	17 million (as of 2019)	National airline; operates a worldwide route network that comprises 78 destinations in 34 countries	Cohort 2
Romania	TAROM	3 million (as of 2018)	Flag carrier of Romania; serves destinations in the Middle East and South Europe	Cohort 2
	Blue Air	5 million (as of 2017)	Low-cost airline; offers flights to 57 scheduled destinations.	
Slovakia	**Danube Wings**	100,000	Regional airline; operates regional scheduled domestic and international flights within Europe	Cohort 1
	Aero Slovakia	n/a	Flag carrier	
Slovenia	**Adria Airways**	600,000	Flag carrier airline,; operates scheduled passenger and charter services to 28 destinations in Europe and the Middle East	Cohort 1
Spain	**Iberia**	20 million (as of 2019)	Flag carrier airline of Spain; operates an international network of passenger and cargo services; flies to over 109 destinations in 39 countries, and a further 90 destinations	Cohort 3

Member State	Main airline(s)	Number of passengers	Number of destinations served	Cohort (assigned)
	Air Europa	9 million	Operates domestic scheduled services and international scheduled services to destinations in Europe, the Mediterranean, Africa (Senegal), North and South America and the Caribbean	
Sweden	**SAS**	See Denmark	See Denmark	Cohort 3
Iceland	**Icelandair**	4 million (as of 2019)	National airline; serves Europe and North America	Cohort 1
Norway	**SAS**	See Denmark	See Denmark	Cohort 3
Liechtenstein	n/a	n/a	n/a	n/a
Switzerland	**Swiss International Air Lines**	19 million (as of 2019)	Flag carrier; operates scheduled services within Europe, to North America, South America, Africa and Asia	Cohort 3
	Edelweiss Air	3 million (as of 2019)	A Swiss leisure airline and the sister company of Swiss International Air Lines; serves various destinations (n=102) in the Mediterranean, in the Caribbean, Kenya and the Maldives, Mauritius, India, Japan and Thailand	

A6.2.3 Additional costs associated with Policy Option 1 (PO1)

This policy option examines the type of mandatory and additional API data fields which carriers would be mandated to transmit to border management and/or law enforcement authorities.

A6.2.4 Scenarios under Policy Option 1

A6.2.4.1 Scenario 1

Scenario 1 relates to the **type of data fields to be collected** for **border and migration management purposes**.

- It includes **a closed and mandatory list of passenger information** to enhance harmonisation and implementation across EU Member States.

- It mandates **aligning future API data elements with MRZ fields and thus aligning with ICAO's PAXLST standards** and **categorise data fields according to their availability and necessity** for **border and migration management purposes**.

- It mandates the **collection of the following additional fields**: **gender**, the **issuing State** or organisation and the **expiration date of the official document**.

- It mandates the **inclusion of scheduled and departure dates as additional fields**. On this point, this scenario also considers **changes to the formulation of flight information should the scope of application of the Directive also be extended to other transport modes** (i.e. formulation of vehicle registration and points of origin and destination)

- This scenario also includes the extension of the personal scope of application of the Directive, namely **collection of data of passengers as well as of crew members**.

- This scenario considers the possibility for national authorities to **request API data from commercial flights only** (the implications of extending this type of requirement from charter flights, cargo and business aviation is assessed in POII).

- This scenario also considers **the standardisation of protocols and data formats** to be used by carriers for the transmission of API data to national authorities and could take the form of an implementing decision attached to the future API instrument. Carriers may still transmit API data using 'old' versions of the PAXLST message, which does not contain for example baggage information fields.

- Lastly, this scenario considers the **processing of API data for public health purposes**.

Similarly, this scenario also mandates the collection and processing of **crew data** by competent national authorities.

A6.2.4.2 Scenario 2

This scenario mandates the colle**ction of the following data fields** <u>in addition</u> to the data elements listed currently in the API Directive and to the mandatory data elements listed in scenario 1:

- Seating information;

- Baggage information (i.e. bag tag identification and checked bag quantity and weight);

- PNR locator number.

A6.2.4.3 Estimation of costs – BMAs and LEAs

The consensus among stakeholders consulted during this study is that PO1 will entail some operational and technical impacts for BMAs. BMAs may be required to modify national API systems and operational guidelines, though with little incidence on organisational changes or staff training. Consultations confirmed that additional data fields would not necessarily require additional staff[289] and, generally, will unlikely affect the API data processing time per passenger.

On the basis that MS already have the necessary infrastructure to collect information against additional fields, we assume that minor changes will be required to MS' infrastructure and equipment owing to small adjustments. We also therefore assume that there will be a small change to maintenance costs.

The table below sets out the main types of costs likely to arise from Scenario 1 and Scenario 2.

A6.2.4.3.1 Additional costs likely to arise from the different scenarios for BMAs and LEAs

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Connectivity /API data exchange capacity	Acquisition / upgrade of communication infrastructure (e.g. link(s) to carriers, EU-LISA carrier gateways, routing of API data flows, link(s) to national watch-list and EU databases, etc.)	On the basis of expert opinion, we have assumed that costs associated with connectivity will increase by 5 to 10%. Estimation was made as follows: *Average (Baseline estimate * 0.05; Baseline estimate *0.1)*
Equipment costs	Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers	On the basis of expert opinion, we have assumed that costs associated with connectivity will increase by 5 to 10%. Estimation was made as follows: *Average (Baseline estimate * 0.05; Baseline estimate *0.1)*
	Acquisition / upgrade of IT business applications / software to process / check API data	Here we have assumed that the cost of IT applications is proportional to the number of data fields to report on. We first looked at data gathered from surveys and consultations on the: - Share of data fields relating to passenger information currently collected vs share of data fields relating to passenger information that will be newly collected - Share of MRZ data fields currently collected vs share of MRZ data fields that will be newly collected

[289] Source: Cost information received from Member States

		- Share of the additional fields: gender, the issuing State or organisation and the expiration date currently covered vs share of the additional fields: gender, the issuing State or organisation and the expiration date that will be newly covered - Share of the additional fields: scheduled and departure dates currently covered vs share of the additional fields: scheduled and departure dates that will be newly covered - Share of crew data currently gathered vs share of crew data that will be newly gathered We then calculated averages to determine the: (i) share of API data fields already covered (%) (ii) share of API data fields that will be newly covered For both BMAs (i.e. Scenario 1) and LEAs (i.e. Scenario 2) Additional costs were finally calculated as: *% of additional fields (average) to be newly covered (BMAs / LEAs) * baseline estimate*
	Redesign of standard operating procedures (for data collection, data access, data processing, data triage and forwarding)	On the basis of expert opinion, we have assumed that costs associated with connectivity will increase by 5 to 10%. Estimation was made as follows: *Average (Baseline estimate * 0.05; Baseline estimate *0.1)*
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Recurring IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was made as follows: *Additional investments * 0.1*
	Costs associated with regular maintenance of business / data applications	
	Costs associated with regular maintenance of communication infrastructure	

A6.2.4.3.2 Estimation of costs – carriers

Impacts on costs for carriers are limited, where additional data elements are within the existing and standardised MRZ fields. Conversely, as pointed out by industry stakeholders, any additional data element required outside of the MRZ will likely:

- imply an adaptation of the check-in systems (mobile, web or kiosk);
- bring about an increase in transmission/ communication costs (owing to larger amounts of data being gathered and transferred).

The evidence gathered does not however point to any substantial increase in staff required to collect and transfer additional data collected (hence no substantial impact on staff costs and/ or staff training costs).

The types of costs likely to be entailed by Scenario 1 and Scenario 2 for carriers are indicated in the table below.

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Equipment/ infrastructure staff costs	One-off investments in upgrade of equipment/ infrastructure	On the basis of expert opinion, we have assumed that costs associated with upgrade of equipment/ infrastructure will increase by 5%. However, in the context of Scenario 2, we can expect economies of scale to accrue to carriers. Compared to Scenario 1 as most of the data fields will already have been covered in Scenario 1. So, we assumed that costs would increase between 1 and 2% under Scenario 2. Estimation was made as follows: *Baseline estimate * 0.05 * total number of airlines flying to/from Member State*
Ongoing communication costs	Cost of "flat-rate" contracts with service providers	We use cost of flat-rate contracts with service providers, for which baseline estimates have been calculated, as a proxy indicator for ongoing communication costs. We assume that these costs will be proportional to the volume of additional data fields to be newly covered. However, based on expert judgment, we assume that costs will rise less than proportionally, i.e. if the share of data fields: - increases by up to 20%: we assume no additional costs - increases by 21-50%: costs increase by 25% - increase by 51-80%: costs increase by 35% - increases by 81-100% and above: costs increase by 50% For Scenario 2, we assume that costs are between 25% and 50% less than those calculated under Scenario 1 owing to the possibility of economies of scale (as discussed above) The calculation of additional costs is therefore as follows:

		*Baseline estimate * relevant % increase in costs * number of air carriers*
Ongoing IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was as follows: *Additional investments * 0.1*

A6.3 Additional costs associated with Policy Option 2 (PO2)

This policy option considers the extension of the scope of API to other flights, covering only air transport. Flights in the scope of each scenario include commercial flights, charter flights, cargo flights and business aviation.

A6.3.1 Scenarios under Policy Option 2

Scenario 1 relates to the introduction of an obligation to **collect API data** systematically for **all extra-Schengen inbound flights** for **border control and migration purposes**.

Scenario 2 relates to the introduction of an obligation to **collect API data** systematically for **all extra-Schengen outbound flights** for **border control purposes and migration purposes**.

Scenario 3 relates to the introduction of an obligation to **collect API data on intra-EU flights for law enforcement purposes**.

Key considerations	Scenario 1	Scenario 2	Scenario 3
Affected group(s)	Air carriers Border Management Authorities (BMAs)	Air carriers BMAs	Air carriers BMAs (data collection/processing) LEAs (data access and use)
Scope of API data collection	All extra-Schengen inbound flights All Member States	All extra-Schengen outbound flights All Member States	Intra-EU inbound and outbound flights All Member States
Relevant scoping variable(s)	MS currently collecting API data on all or some extra-Schengen inbound flights for border control and migration purposes Number/ share of passengers currently subject to API data collection	MS currently collecting API data on all or some extra-Schengen outbound flights for border control and migration purposes Number/ share of passengers currently subject to API data collection	MS currently collecting API data on all or some intra-EU/Schengen flights for law enforcement purposes Number/ share of passengers currently subject to API data collection

A6.3.2 Estimation of costs for BMAs/ LEAs

Based on the operational and technological impacts envisaged by the different scenarios, the following cost items have been estimated for BMAs and/or LEAs.

Additional costs likely to arise from the different scenarios for BMAs and/ or LEAs

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Connectivity /API data exchange capacity	Acquisition / upgrade of communication infrastructure (e.g. link(s) to carriers, EU-LISA carrier gateways, routing of API data flows, link(s) to	We assume that any additional investment in the communication infrastructure will be dependent on the extent of additional routes that will be newly subject to API regulations; hence the extent of

	national watch-list and EU databases, etc.)	additional data collected. We further assume that if the: (1) Scope of the data collection increases by up to 20% → existing systems can cope and therefore there are no additional costs; (2) Scope of the data collection increases by up to 50% → investment is necessary; the increase in costs is assumed to be +25% compared to baseline (3) Scope of the data collection increases by up to 100% → investment is necessary; the increase in costs is assumed to be +50% additional costs compared to baseline The calculation of additional costs is therefore as follows: *Baseline estimate * relevant % increase in costs*
Equipment costs	Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers	Same approach as above
	Acquisition / upgrade of IT business applications / software to process / check API data	
	Redesign of standard operating procedures (for data collection, data access, data processing, data triage and forwarding)	
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Operational staff costs	Costs associated with new / additional management staff	It is difficult to know how many additional staff will be required at each level. We assume that staff levels will be generally dependent on amount of API data being collected (in turn dependent on the number of passengers). We further assume that staff costs will increase less than proportionally with the proportion of additional passengers for whom API data will be collected on each route, i.e If the increase in passengers is up to 20%, we assume current staff levels are sufficient, no additional staff will be needed and no additional staff costs are incurred;
	Costs associated with new / additional IT technical support staff (infrastructure / equipment)	
	Costs associated with new / additional technical support staff (business applications / software)	
	Costs associated with new / additional API data quality controllers (e.g. for reporting and solving data quality issues)	
	Costs associated with new / additional API data analysts (e.g. for processing and dispatching API data)	

		If the increase is between 21% and 50%, a 25% increase in staff is assumed. If the increase is between 51% to 80%, a 35% increase is assumed; and If the increase is 81% and above, a 50% increase is assumed. Costs are therefore calculated as: *Assumed percentage increase in staff * baseline salary estimate*
Recurring IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was as follows: *Additional investments * 0.1*
	Costs associated with regular maintenance of business / data applications	
	Costs associated with regular maintenance of communication infrastructure	

A6.3.3 Estimation of costs for air carriers

Based on the operational and technological impacts envisaged by the different scenarios, the following cost items will be estimated for air carriers.

Additional costs likely to arise from the different scenarios for air carriers

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Equipment costs	One-off costs associated with equipment/infrastructure upgrade/ acquisition	We determined the number of air carriers that would be required to make adjustments to existing equipment/ infrastructure. We use the proportion of flights on which API data are currently collected as a proxy for the number of air carriers currently subjected to API regulations[290]. Additional costs were then calculated as:

[290] We sourced total number of flights on various routes (i.e. domestic, inbound, outbound, etc,) from Eurostat. We also used information gathered from primary research, notably on proportion of routes/journeys on which API data are gathered. We used this data as a proxy for the proportion of flights on which API data are gathered. Data was not available for all MS; hence we calculated averages (based on available data from certain MS) and applied to MS where data were not available

		*(Baseline estimate * number of air carriers that will be newly subjected to API data collection on each route) – (baseline estimate * number of air carriers that are currently collecting API data)*
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Operational staff costs	Additional staff costs	We determined the number of air carriers that would be required to make operational changes. We use the proportion of flights on which API data are currently collected as a proxy for the number of air carriers currently subjected to API regulations versus those that will be newly subjected to API regulations. We assume that costs associated with staff will be proportional to share of passengers for whom API data will be newly collected. However, we assume costs will increase less than proportionally. Where share of passengers is expected to increase by up to 20%, we assume no increase in costs; between 21 and 50%: 25% increase; between 51 and 80%: 35%; and 81% and above: 50%. Operational staff costs will be borne by all carriers. Additional costs are calculated as: *Assumed percentage increase in costs * baseline staff cost estimate*
Ongoing communication costs	Cost of "flat-rate" contracts with service providers	We use cost of flat-rate contracts with service providers, for which baseline estimates have been calculated, as a proxy indicator for ongoing communication costs. We can assume that the cost of flat-rate contracts will increase if the share of passengers whose data are captured increases. We however assume a less than proportional change in costs, i.e. where share of passengers is expected to increase by up to 20%, we assume no increase in costs; between 21 and 50%: 25% increase; between 51 and 80%: 35%; and 81% and above: 50%. We also assume that not all carriers will be subject to the new rules.

		Additional costs are therefore calculated as: *Assumed percentage increase in costs * baseline estimate*
Ongoing IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was as follows: *Additional investments * 0.1*

A6.4 Additional costs associated with Policy Option 3 (PO3)

A6.4.1 Scenario 1

This scenario considers the possibility to impose **an obligation to collect API data to rail carriers**. In practice, two Member States collect API data for from rail carriers for outbound extra-EU journeys: i.e. Estonia and Finland[291]. In France, although national legislation specifies collection of API data from train carriers, the obligation has not been implemented in practice yet[292].

Several aspects are assessed under this scenario, including the types of routes and the purpose for the extension as follows:

S3.1.1. Extending the API obligation to **rail carriers** for **extra-EU inbound routes** for **border management purposes**;

S3.1.2. Extending the API obligation to **rail carriers** for **extra-EU inbound routes** for **law enforcement purposes**;

S3.2.1. Extending the API obligation to **rail carriers** for **extra-EU outbound routes** for **border management purposes**;

S3.2.2. Extending the API obligation to **rail carriers** for **extra-EU outbound routes** for **law enforcement purposes**;

S3.3.1. Extending the API obligation to **rail carriers** for **intra-EU routes** for **border management** purposes;

S3.3.2. Extending the API obligation to **rail carriers** for **intra-EU routes** for **law enforcement purposes**;

S3.4.1. Extending the API obligation to **rail carriers** for **domestic routes** for **border management purposes**; and

S3.4.2. Extending the API obligation to **rail carriers** for **domestic routes** for **law enforcement purposes**.

Scenarios S.3.4.1. and S.3.4.2 have been discarded. The domestic collection of API data has been discarded as this type of requirement can be imposed on carriers solely based on national law and thus, cannot be mandated by a revised API legal instrument.

Scenarios S.3.3.1 and S.3.3.2 have also been discarded. The collection of passenger data for intra-EU journeys contravenes the principle of free movement of persons within the Schengen area.

A6.4.1.1 Estimation of costs for BMAs and LEAs

Additional API data collection will likely require an upgrade in BMAs/LEAs' communication infrastructure to include new carrier types. New or upgraded equipment may also be required. With additional data to process, additional staff may also be needed.

The main affected cost categories, along with the method for calculating/ estimating additional costs, are set out below.

Cost category	Sub cost category	Methodology
Connectivity	Upgrade of communication infrastructure	We first looked at which Member States currently serve passengers on the routes within scope.

[291] As per the Evaluation

[292] Articles L232-1 and L232-4 of the Internal Security Code

		We then looked at the share of passengers for whom API data are currently collected on each relevant route. We calculated the (expected) average increase in passengers subjected to API data collection. We assumed that costs associated with the upgrade of the communication infrastructure would increase less than proportionally with the share of passengers who will be newly subjected to API data collection. Where the expected increase is up to 50%, additional connectivity costs are assumed to increase by 25%; if the increase is more than 50%, costs are assumed to increase by 50%
Equipment costs (one-off)	Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers	Some Member State authorities have indicated that the main equipment costs likely to be affected are: acquisition/upgrade of IT equipment; and acquisition/ upgrade of IT business applications. These MS have provided cost estimates. We used these to calculate estimates for MS in different clusters. The clusters are the same as those listed in the baseline. Small MS: (BG, EE, HR, HU, LU, RO, SI, SK): we assume that costs are half of that for medium MS, i.e. (228,000/2) = EUR 114,000 Medium MS: (AT, BE, CZ, DK, FI, IE, LT, LV, MT, NL, PL, PT, SE, CH) – the average of costs provided by Belgian and Swedish authorities is calculated as: (375,000+80,000/2) = EUR 228,000 and used for MS within this cluster Large MS (FR, ES, DE, IT) – the average provided by Italian authorities, i.e. EUR 1,500,000 is assigned to MS within this cluster

	Acquisition / upgrade of IT business applications / software to process / check API data	Same approach as above. Here estimates (based on data gathered from BMAs/ LEAs) are as follows: Small MS: (BG, EE, HR, HU, LU, RO, SI, SK): we assume that costs are half of that for medium MS, i.e. (228,000/2) = EUR 114,000 Medium MS: (AT, BE, CZ, DK, FI, IE, LT, LV, MT, NL, PL, PT, SE, CH) – the average of costs provided by Belgian and Swedish authorities is calculated as: (375,000+80,000/2) = EUR 228,000 and used for MS within this cluster Large MS (FR, ES, DE, IT) – the average provided by Italian authorities, i.e. EUR 1,500,000 is assigned to MS within this cluster
Operational staff costs (recurring)	Costs associated with new / additional IT technical support staff (infrastructure / equipment)	For costs associated with new / additional IT technical support staff (infrastructure / equipment), we assume that staff costs are proportional to the number/ share of passengers who will be newly affected by API obligations. We however assume costs to increase less than proportionally with an increase in the share of passengers who will be newly subject to API data collection. Hence, we assume an increase of 25% in costs, where the share of passengers increases by up to 50%; and an increase of 50% where the increase in share of passengers is between 51% and 100%. Additional costs are therefore calculated as: 0.25*baseline estimate or 0.5*baseline estimate.
	Costs associated with new / additional technical support staff (business applications / software)	Estimates were provided by Italian authorities, which appeared feasible. We assumed that the minimum value (estimated by the authorities) of EUR 800,000 applies to MS within the small cluster; the maximum value of EUR 1,400,000 to MS within the large cluster; and the average of (800,000+1,400,000/2) = EUR 1,100,000 to MS within the medium cluster Additional costs are then calculated as: new estimated costs *minus* baseline costs
	Costs associated with new / additional API data quality controllers (e.g. for reporting and solving data quality issues)	Estimates were provided by Italian authorities, which appeared feasible. We assumed that the minimum value (estimated by the authorities) of EUR 80,000 applies to MS within the small cluster; the maximum value of EUR 160,000 to MS within the large cluster; and the average of (80,000+160,000/2) = EUR 120,000 to MS within the medium cluster

		Additional costs are then calculated as: new estimated costs *minus* baseline costs
	Costs associated with new / additional API data analysts (e.g. for processing and dispatching API data)	Estimates are provided by Italy, which appear feasible. We assume that MS within the small cluster experience the minimum level of costs estimated by Italian authorities, i.e. EUR 400,000; MS within the large cluster EUR 700,000; and MS within the medium cluster the average of (400,000+700,000/2) = EUR 550,000 Additional costs are then calculated as: new estimated costs *minus* baseline costs
Ongoing communication / connectivity costs	Costs of connectivity with carriers / EU LISA	BMAs/ LEAs consulted indicated additional costs of connectivity with carriers. Estimates were provided by Belgium and Sweden, which appear feasible. We assume that MS within the small cluster experience the minimum level of costs estimated by Italian authorities, i.e. EUR 400,000; MS within the large cluster EUR 700,000; and MS within the medium cluster the average of (400,000+700,000/2) = EUR 550,000 Additional costs are then calculated as: new estimated costs *minus* baseline costs
	Other data exchange fees	
Recurring IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was as follows: *Additional investments * 0.1*
	Costs associated with regular maintenance of business / data applications	
	Costs associated with regular maintenance of communication infrastructure	

A6.4.1.2 Estimation of costs for rail carriers

Consulted stakeholders, including BMAs and LEAs and industry representatives and rail carriers agree that a potential extension of the scope of API would require one-off investments, in terms of set-up costs. Hiring of additional personnel may also be required as well as staff training.

The main affected cost categories, along with the method for calculating/ estimating additional costs, are set out below.

Cost category	Sub cost category	Methodology
One-off investments	Set-up costs	We first determined which Member States currently receive inbound and outbound extra-Schengen passengers via rail, sea and coach/bus. Where MS do not, we assume set-

		up costs will be zero as carriers will unlikely receive passengers on these routes in the future and will not have to collect API data. Where MS receive passengers on the said routes, we assume that at least half will be affected by API data collection. We also assume that at least half of total rail/maritime/coach carriers will be affected (as not all carriers will be operating the said routes). We use baseline estimates obtained for air carriers. We assume that average set-up costs for one carrier in the maritime/ rail/ land transport sectors are at least on par with those estimated for one carrier in the air transport sector. Costs are therefore calculated as follows: Cost per carrier X total number of (affected) carriers in each sector
Operational costs	Staff costs	We assume that staff costs will be influenced by passenger levels. We first calculate ratios of the number of passengers affected by API in the air transport sector to the number of passengers (likely to be) affected in each of the other transport sectors. We use the ratios to calculate approximate total staff costs in the other transport sectors. We exclude MS which do not currently receive passengers on inbound and outbound extra-EU/Schengen routes as they are unlikely to receive passengers on these routes in the future. To calculate total staff costs in each MS for (concerned) rail/maritime/coach carriers, we use the following approach: Ratio of affected passengers (air): *N_r= Affected rail passengers / currently affected air passengers* Total costs in each MS (rail carriers) = total costs (observed for air carriers) X n_r We repeat the above calculations for the other transport sectors within scope. Please note that for MS that are already gathering API data from rail/maritime/coach

		carriers on some extra-EU routes, we assume zero to marginal costs as it is unlikely that full set-up costs would be required by carriers in those MS as they are already collecting the necessary information.
Ongoing communication costs	Costs – flat-rate contracts	We assume that cost of contracts will increase with the number of passengers for whom API data will be collected. As we are using estimates obtained for air carriers, we calculate ratios to check differences in passenger levels across the different transport sectors. The ratio obtained (e.g. n_r: for rail carriers) is then used to estimate per carrier cost in the transport sectors concerned as follows: Average cost (rail): average cost (air carrier) / n_r: We then multiply by total number of affected carriers in each sector to obtain total additional costs, e.g. Total cost: average cost x affected rail carriers
Ongoing infrastructure/ equipment costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	As investments will be made in equipment and other infrastructure by carriers, we can assume that maintenance will be needed. Expert opinion suggests that maintenance costs will likely amount to about 10% of initial investments. Additional cost: additional investments x 0.1 Total additional cost: additional cost x number of affected carriers
	Costs associated with regular maintenance of business systems / data applications (DCS, CRS, ID biometric systems, etc.)	

A6.4.2 Scenario 2

This scenario considers the possibility to impose an obligation to collect API data to water-borne carriers (i.e. maritime carriers).

Several aspects are assessed under this scenario, including the types of routes and the purpose for the extension as follows:

- Extending the API obligation to **water-borne carriers** for **extra-EU inbound routes** for **border management purposes**;
- Extending the API obligation to **water-borne carriers** for **extra-EU inbound routes** for **law enforcement purposes**;

- Extending the API obligation to **water-borne carriers** for **extra-EU outbound routes** for **border management purposes**;
- Extending the API obligation to **water-borne carriers** for **extra-EU outbound routes** for **law enforcement purposes**;
- Extending the API obligation to **water-borne carriers** for **intra-EU routes** for **law border management purposes**;
- Extending the API obligation to **water-borne carriers** for **intra-EU routes** for **law enforcement purposes**;
- Extending the API obligation to **water-borne carriers** for **domestic routes** for **border management purposes**; and
- Extending the API obligation to **water-borne carriers** for **domestic routes** for **law enforcement purposes**.

The scenarios highlighted in red above are excluded.

A6.4.2.1 Estimation of costs for BMAs and LEAs

Please refer to the approach discussed under Scenario 1.

A6.4.2.2 Estimation of costs for maritime carriers

Please refer to the approach discussed under Scenario 1.

A6.4.3 Scenario 3

This scenario considers the possibility to impose an obligation to collect API data to overland coach carriers.

Several aspects are assessed under this scenario, including the types of routes and the purpose for the extension as follows:

- Extending the API obligation to **coach carriers** for **extra-EU inbound routes** for **border management purposes**;
- Extending the API obligation to **coach carriers** for **extra-EU inbound routes** for **law enforcement purposes**;
- Extending the API obligation to **coach carriers** for **extra-EU outbound routes** for **border management purposes**;
- Extending the API obligation to **coach carriers** for **extra-EU outbound routes** for **law enforcement purposes**;
- Extending the API obligation to **coach carriers** for **intra-EU routes** for **law border management purposes**;
- Extending the API obligation to **coach carriers** for **intra-EU routes** for **law enforcement purposes**;
- Extending the API obligation to **coach carriers** for **domestic routes** for **border management purposes**; and
- Extending the API obligation to **coach carriers** for **domestic routes** for **law enforcement purposes**.

The scenarios highlighted in red above are excluded.

A6.4.3.1 Estimation of costs for BMAs and LEAs

Please refer to the approach discussed under Scenario 1.

A6.4.3.2 Estimation of costs for coach carriers

Please refer to the approach discussed under Scenario 1.

A6.5 Additional costs associated with Policy Option 4 (PO4)

This policy option considers improvements in the quality of API data collected. The scenarios considered are discussed below.

A6.5.1 Scenario 1

Scenario 1 considers **mandating automated collection of API data,** so as to **eliminate manual entry at check-in and online self-declaration** of API data by the passenger.

This would entail **the capture of API data from the MRZ through automated means – presently with devices using technologies, such as optical character recognition (OCR) or infrared light**.

The collection of **additional information on secondary travel documents** (for bi-nationals or when other travel documents have been used such as Residence Cards and Residence Permits) **could also be considered, provided they have an MRZ**.

In the case of in-person check-in, this would imply that **carriers should scan the MRZ of the document**. In the case of online check-in, this would imply that individuals checking in should use a mobile phone app to scan the MRZ – such apps are already widely available, and some carriers have implemented them.

A6.5.1.1 Scenario 2

There are two aspects to this scenario:

- First, it aims to further ensure the quality and the authenticity of MRZ data, by mandating carriers to compare it with the information in the traveller document’s RFID chip;
- Second, it establishes the legal grounds allowing carriers to use the biometric data from the RFID chip (e.g. facial image), to verify that API data extracted during the (self) check-in process corresponds to the passenger boarding the plane (or other mode of transportation).

A6.5.1.2 Estimation of costs – BMAs/ LEAs

The automated collection of API data will likely require the modification of BMAs’ API systems/ equipment. However, there seems to be differences in expected costs between two groups of Member States, depending on their current systems. Half of the institutions (BE, FI, IT, SE) responding to the BMA and LEA survey believe that the automated collection of API data will entail costs, while the other half (CH, LT, LU, SI) do not believe there will be such effects.

We have thus assumed that BMAs / LEAs will not be engaged in additional data capture and therefore, will unlikely bear major costs. We assume that investments in new tools to check API data quality may nonetheless have to be made. Other costs are assumed to stem from a redesign of standard operating procedures.

Finally, we assume that no additional staff costs will arise. We assume that PO4 will be cost neutral when it comes to staff costs. As such, with better quality data obtained from carriers, there will likely be less interaction/ follow-ups required with carriers or less time required to correct errors. There would therefore be important time savings for BMAs/LEAs. However, it can be argued that part of these efficiency gains will be "lost" as staff gets redeployed to other internal activities.

The table below sets out the main types of costs likely to be incurred by BMAs/ LEAs as a result of the different scenarios.

Additional costs likely to arise from the different scenarios for BMAs/ LEAs

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Equipment costs	Acquisition / upgrade of IT equipment (i.e. hardware) to collect the data from carriers	Some estimates have been provided by a few Member States (MS) (BE, FI, IT and SE). We use these estimates and apply to different clusters of MS, i.e. - small MS (BG, EE, HR, HU, LU, RO, SI, SK); - medium MS (AT, BE, CZ, DK, FI, IE, LT, LV, MT, NL, PL, PT, SE, CH); - large MS (FR, ES, DE, IT). We attribute the lowest average of EUR350,000 (gathered across the MS authorities) to MS within the small cluster; the highest average of EUR950,000 to MS within the large cluster; and the average of EUR 650,000 to MS within the medium cluster. Additional costs across MS is then calculated as: *New estimated cost minus baseline cost estimate*
	Acquisition / upgrade of IT business applications / software to process / check API data	Some estimates have been provided by a few MS (BE and SE). We attribute the lowest average of EUR500,000 (gathered across the MS authorities) to MS within the small cluster; the highest average of EUR600,000 to MS within the large cluster; and the average of EUR 550,000 to MS within the medium cluster. Additional costs across MS is then calculated as: *New estimated cost minus baseline cost estimate*
	Redesign of standard operating procedures (for data collection, data access, data processing, data triage and forwarding)	On the basis of expert opinion, we assume that costs stemming from a redesign of operating procedures will increase by 10% Additional costs are calculated as follows:

		*Baseline estimate * 0.1*
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Recurring IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in infrastructure costs. Estimation was as follows: *Additional investments * 0.1*
	Costs associated with regular maintenance of business / data applications	

A6.5.1.3 Estimation of costs – carriers

The set of processes for capturing API data will impact on carriers' capital and operational expenditures as a resulting of having to:

- Invest in more equipment (e.g. to read MRZ);
- Modify and upgrade their existing software and hardware infrastructure (e.g. develop new mobile phone applications;
- Modify their operational set-up to render possible the capture of passenger information, its aggregation and transmission.

A6.5.1.3.1 Specific considerations

- The air-carriers survey indicated, though, that **very few carriers (4 out of 20) exclusively rely on the use of the Optical Character Recognition (OCR) for extracting the data from the Machine-Readable Zone (MRZ) of travel documents**. The methods are usually mixed and include self-declaration of passengers via an app / website (9 out of 20), and manual collection by staff (9 out of 20).
- **About 57% of global passengers are already offered with the possibility of doing self-boarding** (either by scanning their document or through automatic doors).
- **Web/mobile check-in option is not universally accepted in all countries outside the EU**. Nevertheless, **countries representing 95.84% of all global passengers accept mobile check-in, and these countries – 'swiping' could be done at check-in**[293].

The types of costs likely to be entailed by the different scenarios for carriers are indicated in the table below.

Cost category	Sub cost category	Methodology
One-off costs, i.e. fixed or variable costs paid only once		
Equipment costs	Upgrade of equipment	Here we have gathered data on: - the share of airlines which currently use automated solutions (e.g. OCR) for API data collection/ transmission.

[293] According to data presented by IATA for the present study.

		The carriers' survey indicates that 4 out of 20 carriers are currently collecting API data via automated means. Our general assumption is therefore that at least (4/20*100) = 20% of carriers in each MS currently collect data via automated means - the share of airlines which currently undertake RFID verification On the basis of evidence gathered, it appears that this is close to 0 in most MS We then assume that, where air carriers already have some form of automation in place, we assume that costs will rise by about 25%. Where no automated solutions are used by air carriers, we assume costs will rise by 50% Additional costs are then calculated as: *Estimated percentage increase in costs * baseline estimate * number of air carriers*
Recurring costs, i.e. fixed or variable costs paid at regular intervals		
Operational costs	Additional staff costs	Air carriers will have to modify their operational set-up to render possible the capture of passenger information, its aggregation and transmission. We therefore assume some degree of change in operational staff costs. We assume that staff costs will be proportional to the volume of passengers who will be subject to automatic collection of their data; however, we assume costs will increase less than proportionally. Where share of passengers is expected to increase by up to 50%, we assume an increase in costs of 25%; where the share is expected to increase by 51% or more, we assume an increase in costs of 50%. Additional costs are then calculated as: *Estimated percentage increase in costs * baseline estimate * number of air carriers*
Ongoing communication costs	Cost of "flat-rate" contracts with service providers	We assume that the cost of flat-rate contracts will increase if the share of passengers whose data are captured increases. We however assume a less than proportional change in costs, i.e. if the share of passengers increases by up to 50%, the

		increase in costs is estimated at 25%; if the share increases by 51% or more, the increase in costs is estimated at 50% Additional costs are then calculated as: *Estimated percentage increase in costs * baseline estimate * number of air carriers*
Ongoing IT infrastructure costs	Costs associated with regular maintenance of IT equipment and other related infrastructure	On the basis of expert opinion, we have assumed that maintenance costs will be about 10% of the additional investments in equipment and infrastructure costs. Estimation was as follows: *Additional investments * 0.1*
	Costs associated with regular maintenance of business systems / data applications (DCS, CRS, ID biometric systems, etc.)	

A6.6 Additional costs associated with Policy Option 5 (PO5)

This option examines the possibility of streamlining the transfer of API data between carriers and national authorities (NAs) by reusing the carrier interface defined under EES(VIS) and ETIAS Regulations. The interactive query that is planned for the ETIAS and EES system will in fact use (a subset of) API data and the air carriers' interactive API IT/communication infrastructure. As a result, the Carrier Gateway (CG) for EES and ETIAS sets a foundation for a centralised point of communication for all air carrier API data for European destinations.

A6.6.1 Scenario 1

This scenario considers **upgrading the Carrier Gateway (CG) with the CRM technical capabilities** allowing carriers to send API data to national authorities through a central point following the Single Window approach.

The technological and operational implications of Scenario 1 will be as follows:

- As the usage of API (batch) data remains the same, there will be no major investments needed at protocol or file transfer level.
- Current implementations of national systems can continue to operate API batch and need to manage only one interface to receive the information.
- Carriers will need to connect their systems to the CRM only as opposed to that of Member States' separately.

A6.6.1.1 Estimation of costs – BMAs/ LEAs

There will unlikely be any significant costs associated with Scenario 1. This is because most MS already have existing communication infrastructure and other equipment in place to communicate/ deal with eu-LISA.

A6.6.1.1.1 Potential cost savings

In addition, Scenario 1 will likely confer cost savings to BMAs/ LEAs. As such, there will be only one connection to manage, which will be the connection to eu-LISA's centrally-hosted CRM/CG interface for the transmission and receipt of data. We can thus assume that cost savings will ensue from reduced staff time spent on communication with individual carriers.

Nonetheless, within BMAs/ LEAs, these cost savings may be limited as it can be expected that staff no longer engaged in communication with carriers will be reassigned to the task of managing the eu-LISA single interface and/or other internal activities.

Scenario 1 is therefore assumed to be a cost neutral option for BMAs/LEAs.

A6.6.1.2 Estimation of costs – EU agencies (i.e. eu-LISA)

EU agencies, notably EU-LISA, can expect an increase in development costs, i.e. investments in:

- IT infrastructure and licenses
- Solution development
- Solution deployment

The CRM Feasibility Study (January 2019) assessed whether a CRM that handles both the Interactive Query and Batch API and PNR messages would be beneficial. The "Resource Requirements Report" created as part of that study provided a cost model, which detailed the costs of developing and operating the Carrier Interface which would support the Interactive Query for EES/ETIAS. The cost of implementing this solution was referred to as the "baseline cost". Also presented in this cost model were a number of "What-if" scenarios, one of them specifically estimating the incremental cost of routing Batch API/PNR through the Carrier Interface. This is the estimate which is used below.

There are two main cost elements relevant to the API study that can be derived from the CRM cost model:

Costs associated with transferring the EES/ETIAS carrier gateway to a Central Routing Mechanism (CRM) system. This covers the development and deployment of the CRM services as an extension of the ICT built for EU-LISA's EES/ETIAS Carrier Interface.

Costs associated with an increase of the ICT infrastructure capacity to process more passengers as it is the case for policies requiring more NAs receiving APIs, more flights, more carrier operators, or more passengers.

At this stage, there is not enough information available to determine if extra costs reduction, compared to the CRM study, are possible on the basis that some of the CRM components would be shared with the eu-LISA Carrier Gateway under construction.

Cost estimates from the CRM feasibility study are as follows (and can be used in the context of development and operational costs for EU-LISA):

Type of cost	CRM Developer	CRM Operator
Acquisitions and development		
IT infrastructure and licenses	**EUR 2,382,000**	**-**
Solution development	EUR 2,564,000	EUR 224,000
Solution deployment	EUR 260,000	EUR 1,605,000
Acquisitions & development (total)	***EUR 5,206,000***	***EUR 1,829,000***
Operational costs (per year for 5 years)		
Infrastructure – support and maintenance	EUR 793,000	-
Operations support	EUR 287,000	EUR 815,000
Operational costs (total)	***EUR 1,080,000***	***EUR 815,000***

The number of passengers/year that are reported in the API messages is one of the basic CRM sizing parameters. It determines the capacity in ICT resources to process the messages associated to each passenger travel.

The CRM study cost estimation calculator leads to a cost per additional million passengers/years. The CRM baseline costs is based on 285 million passengers/year. The estimate of costs associated to an increase of passengers is derived from the CRM cost model by doubling the number of passengers of the baseline scenario, and determining the costs increase per million passengers. This amounts to:

Yearly infrastructure additional costs: EUR 4,300 per million passengers;

Yearly infrastructure IT support and maintenance additional costs: EUR 1,075 per million passengers.

Frontex will also likely have to bear additional staff costs owing to the management of communication with carriers (and Member States authorities). In other words, the task of managing API data collection from carriers will now be transferred from BMAs/LEAs to EU-LISA. It is difficult to estimate how many staff members will be recruited by the agency. It is therefore assumed that Frontex will bear an equivalent of 20% to 50% of staff costs currently borne by BMAs/ LEAs.

A6.6.1.3 Estimation of costs – carriers

With the CRM/CG interface, carriers will no longer have to manage multiple connections. They will be required to manage only one connection with eu-LISA. We can therefore envisage a reduction in costs as less staff will likely be required for the management of connections. Still, some carriers may want to retain communication links with (some) Member States. In addition, staff may be reassigned to other duties related to the management of communications with eu-LISA and/ or other internal activities.

Scenario 1 is therefore assumed to be cost neutral option for carriers.

A6.6.2 Scenario 2

This scenario examines the possibility of transmitting API data to national authorities at the same time as it is received for the query of the EES/ETIAS database (typically at the moment of check-in), which removes the need for the transmission of batch API and/ or exchange of iAPI by carriers. It further supports the SW approach by enabling the API data transfer through the CRM/CG using a single protocol (iAPI) and timing (during check-in).

A6.6.2.1 Estimation of costs – BMAS and LEAs

We assume that similar cost savings observed under Scenario 1 will apply here. Cost savings will arise from the reduction in communication links to manage. Hence, staff costs will fall, though staff members no longer managing communication links with carriers may be reassigned to the management of communications with eu-LISA and/ or other internal activities. We can therefore assume that Scenario 2 will be cost neutral for BMAs/LEAs.

A6.6.2.2 Estimation of costs – EU agencies (i.e. eu-LISA)

As under Scenario 1, EU agencies, notably EU-LISA, can expect an increase in development costs. The methodology used is the same as the one set out under Scenario 1. We assume the costs will be cumulative and expect another 10% in development and operational costs. We do not expect EU-LISA having to bear additional staff costs as this Scenario mainly impacts the evolution and further development of the interface.

Additional costs under Scenario 2 can be calculated as:

*0.1*initial development costs (Scenario 1)*

A6.6.2.3 Estimation of costs – carriers

The removal of the need for sending batch data as part of Scenario 2 will likely confer other cost savings to carriers, notably in the form of reduced communication costs. Carriers will also likely save on staff costs, given that fewer staff members will be required to spend time on the management of communication links with Member States. However, these resources may be redeployed to other activities internally.

Additionally, carriers may be required to invest in iAPI functionalities, which would generate additional costs.

All in all, it is therefore assumed that this scenario will be cost neutral for carriers, owing to cost savings being on par (or outweighed) by additional costs elsewhere.

A6.6.3 Scenario 3

This scenario examines the possibility of enabling national authorities' systems to complement the iAPI return message to carriers by sending a response through secondary processing. As such, the system within each MS, which receives the iAPI data, can complement an interactive reply – within a 4 seconds window – using information found in national databases, such as watchlists, to allow or deny entry of a TCN.

A6.6.3.1 Estimation of costs – BMAs and LEAs

Scenario 3 will have the following cost implications for BMAs/ LEAs:

- Member States' systems will need to be adapted, such that an interactive 4 seconds response window can be achieved to send back complementary messages to carriers on a per-traveller basis.

To calculate the extent of adaptation or development costs, we assume that infrastructure and equipment costs will increase by about 10% to 50%. This is in part based on data available from the CRM study which posits that the overall incremental costs for enabling an extension of the CRM/CG for iAPI (i.e. costs associated with system adaptation, such that it becomes more interactive) are relatively low (about 13% of increase related to the baseline total estimated costs).

Additional development costs for BMAs/ LEAs will therefore be calculated as:

*Average [(0.1 * baseline estimate (for equipment-related costs)); 0.5 * baseline estimate (for equipment-related costs)]*

Additional staff may be required to process the data received. However, given that less staff will be engaging in the management of communication links with individual carriers, we can expect that they will be reassigned to additional/ new tasks entailed by Scenario 3. Hence, we assume no additional staff costs.

A6.6.3.2 Estimation of costs – EU agencies (i.e. eu-LISA)

As under Scenario 1 and Scenario 2, EU agencies, notably EU-LISA, can expect an increase in development costs. The methodology used is the same as the one set out under Scenario 1. We assume the costs will be cumulative and expect another 10% in development and operational costs (in addition to those experienced under Scenario 2). We do not expect EU-LISA having to bear additional staff costs as this Scenario mainly impacts the evolution and further development of the interface.

Additional costs under Scenario 2 can be calculated as:

*0.1*total development costs (Scenario 2)*

A6.6.3.3 Estimation of costs – carriers

Scenario 3 will unlikely entail significant costs for carriers as the changes envisaged are mainly directed at national authorities and EU-LISA.

A6.6.4 Scenario 4

This scenario considers the use of the centralised API flow via the CRM to query other central data bases than EES and ETIAS, and to complement the API information sent to the NAs with alerts generated from central checks. For example, once the European Search Portal (ESP) becomes available, the API can be used to perform adequate searches and forward the findings to the relevant NAs.

The scenario also considers a mechanism for the API data to interact with a central risk-analysis system, leveraging data analytics to get an EU-wide picture of the API data streams.

A6.6.4.1 Estimation of costs – BMAs and LEAs

We expect Scenario 4 to be cost neutral for BMAs/ LEAs as most of the activities conducted by staff within national authorities (e.g. checks against relevant databases) will now be transferred over to staff within EU-LISA. Although there will be a reduction in staff costs within BMAs/ LEAs, we can expect that staff will be re-assigned to other activities (e.g. additional checks on national databases, more risk and situational analyses). Hence, the notion of cost neutrality.

A6.6.4.2 Estimation of costs – EU agencies

There may be additional staff costs for EU-LISA. As stated above, staff within EU-LISA will be taking over various activities previously carried out by staff within national authorities.

It is difficult to estimate how many staff members will be recruited by the agency. It is therefore assumed that EU-LISA will bear an equivalent of 20% to 50% of staff costs currently borne by BMAs/ LEAs.

A6.6.4.3 Estimation of costs – carriers

The future centralised business application that requires API data for performing their business purpose will benefit from API data available via an interoperable system (CRM) through a significant reduction of their development costs.

(A description of the benefits of centralised compliance checking and risk/targeting is beyond the scope of the study).

Cost estimations are not provided as this is a vision of the ultimate purpose of collecting API data on a EU wide scale.

Annex 7 Survey analysis

Please see separate document.

Annex 8 Evidence annex

Please see separate document.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696, or

— by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: https://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (https://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union