Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82

Final Report for Directorate-General for Home Affairs

Written by

Home Affairs

This document has been prepared for the European Commission. 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.

Document control

Document Title	Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82
Prepared by	Emanuela Canetta, Silja Korpelainen, Camino Mortera, Laura Robson, Veronika Minkova, Konstantinos Damianakis
Checked by	Mathieu Capdevila
Date	17 September 2012

Contents

1 Introduction

This Final Report presents the results of the evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set by Directive 2004/82, an assignment that has been carried out by ICF GHK in partnership with Milieu, on behalf of DG Home Affairs.

The report aims to provide an overview of the activities undertaken and well as report on the findings of the study.

In particular, the main purposes of this report are to:

- Present conclusions of the assignment, based on the results of desk research, interviews and surveys with key stakeholders at national level (e.g. Border Management Authorities, Law Enforcement Authorities, Data Protection Authorities, Air carriers) and at international level (airline industry representatives and international organisations),
- Present the findings concerning the quality of the transposition and implementation of the Directive in Member States[1]
- Present the findings concerning the relevance and coherence, effectiveness and efficiency, impact and added value,
- Formulate conclusions and recommendations, and,
- Provide the mapping of the legislation and an overview of the implementation of the Directive in the Member States

1.1 Aims and objectives of this study

The aim of this study is to provide the Commission with key findings regarding the implementation and functioning of the national measures taken by Member States to comply with Directive 2004/082/EC of 29 April 2004; the end goal of the Commission being to present a report to the European Parliament and the Council on the level of compliance with and extent of the transposition of the Directive.

More specifically, the study allows the Commission to assess the results and impacts of the Directive, to identify best practices on the basis of current experiences and to examine adjustments needed to overcome possible obstacles in the use of API data. The study reveals whether the current legal provisions and procedures put in place have delivered the intended results and whether these results have been achieved in the most efficient way possible.

Particular emphasis was given to the relevant experiences and statistics from Member State authorities and carriers enabling to assess the usefulness of API and to identify possible gaps.

1.2 Structure of this report

The remainder of this Report is structured as follows:

- Section 2 – Executive summary
- Section 3 – Overview of study methodology
- Section 4 – Overview of the Directive
- Section 5 – Analysis of the quality of the transposition
- Section 6 – Analysis of the quality of the implementation
- Section 7 – Results and impacts of the Directive
- Section 8 – Conclusions and recommendations

[1] The Member States cover EU27 and Iceland, Norway, Switzerland and Liechtenstein.

2 Executive summary

This is the Final Report on the evaluation of the implementation and functioning of the obligation of carriers to communicate passenger data as of Directive 2004/82/EC. This executive summary provides an overview of the main findings of the study.

2.1 Introduction and policy context of the evaluation

The aim of the study is to provide the European Commission with key findings regarding the implementation and functioning of the national measures taken by Member States to comply with Directive 2004/082/EC of 29 April 2004.

The focus of the study is to allow the Commission to assess the results and impacts of the Directive, to identify best practices on the basis of current experiences and to examine adjustments needed to overcome possible obstacles in the use of API data. The study explores the extent to which the current legal provisions and procedures put in place have delivered the intended results and whether these results have been achieved in the most efficient way possible.

The overall objective of the study is provide the necessary information to enable the Commission to present a concise, factual and evidenced report to the European Parliament and the Council on the implementation and functioning of the Directive.

2.2 Methodology

A mixed-method approach has been implemented to enable the triangulation of evidence using qualitative and quantitative approaches. The study has focussed on assessing the (i) quality of the transposition of the Directive, (ii) the quality of the implementation of the Directive and (iii) the results, impacts and added value of the Directive. To assess the outcomes and results of the application of the Directive, the key evaluation criteria of Relevance, Effectiveness, Efficiency, Impact and Added Value have been used, supported by a set of clear evaluation questions. The three phases of the study, from inception, collection of data and its analysis through to conclusions and recommendations were designed to specifically address these evaluation questions.

The study performed a conformity checking exercise on the relevant measures in each Member State to conclude the overall quality of the transposition. The overall quality of the transposition was assessed on the following basis: whether (i) the transposition was judged to be in full conformity with the Directive and hence in line with *all* its requirements or (ii) whether the non-conformity was judged to be as a result of an incomplete and/or incorrect transposition.

The study also investigated which Member States have implemented the Directive in practice, and therefore established relevant API systems. Where this was the case, including the pilot systems in operation, an analysis of the quality of the implementation was undertaken, which concerned 19 Member States. Overall, 72 interviews were conducted as part of the study including national and international stakeholders, border management authorities, Ministries of Interior and Transport, Data Protection Authorities, air carriers and international organisations. Two online surveys were also launched as part of the study, directed to national competent authorities and air carriers.

The results have been analysed and synthesised using quantitative and qualitative techniques.

2.3 Overview of the Directive

The Directive 2004/82/EC on the obligation of carriers to communicate passenger data (known as the API Directive) was adopted on 29 April 2004. The Directive has two main aims, namely (1) improving border controls and (2) combating illegal immigration. In addition, the Directive permitted Member States to use the API data for law enforcement purposes to a certain extent and under certain conditions. For the purposes of this study, 'law

enforcement' has been considered in light of Recital 12 of the Directive.[2] For more information about the interpretation of this expression, see section 5.2.7 below.

In order to achieve the above mentioned aims, the Directive requires carriers to communicate information on passengers travelling from a third country to a European Member State to the relevant national authority in charge of border checks at the external border, at the time of passenger check-in.

Such information is referred to as Advanced Passenger Information (API), and includes data which allows for the identification of the passenger, his/her travel documents, incoming flight, destination and time of departure and arrival.

Data transmission, processing and retention obligations applying to carriers (and national authorities) are specified, and sanctions for carriers are foreseen in cases of infringements.

2.4 Quality of transposition and implementation

2.4.1 Analysis of the quality of transposition

The analysis of the compliance of the national transposition measures with the obligations of the Directive has been carried out by following a formalistic approach to allow the identification of any issue of conformity. However, when the issues of conformity in the transposing legislation do not correspond to problem in the overall national legal system and/or in practice, the situation has been qualified as 'minor problem' and an explanation for such assessment is provided. The result of this analysis is that some transposition issues were identified but only few had an impact in practice.

All Member States have transposed some or all the provisions of the Directive.[3] However, the vast majority of Member States' legislation is not in full conformity with the Directive. While one Member State[4] is in full conformity, eight Member States[5] are not due to gaps in transposition, two Member States'[6] have incorrectly transposed some of its provisions and the remaining 18 Member States[7] have incorrectly and not fully transposed all of the provisions of the Directive.

The main issues of non-conformity relate to:

- Data protection legislation: potential issues related to provisions on the length of retention of API data by authorities and carriers. The lack of cross-reference to EU and/or national data protection legislation for 22 Member States does not cause a problem in practice as all Member States have data protection legislation in force[8,9].
- Late transposition: 17 Member States transposed the Directive later than the deadlines laid down by Article 7,[10]
- Gaps in the definitions: only two Member States included all the definitions contained in Article 2 of the Directive in their transposing legislation[11]. However, in some cases the

[2] Recital 12 reads '(…)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 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.

[3] The above assessment is not applicable to Denmark, since Denmark is not bound to transpose the Directive under EU law. In addition, Liechtenstein has not been considered in the analysis of the transposition of the Directive since it does not have an airport or any external land or maritime borders.

[4] SI

[5] BG, CY, FR, ES, IE, NO, RO and SE.

[6] EL and LV.

[7] AT, BE, CH, CZ, EE, FI, DE, HU, IS, IT, LT, LU, LV, MT, PL, PT, SK and the UK.

[8] AT, BG, CH, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, IT, IS, LT, LV, NO, PL, SE, SK and the UK.

[9] For a more detailed analysis of the data protection issues relating to both national authorities and carriers, please, see section 5.2.6.

[10] The deadline for transposition was the 5 September 2006.

definitions are contained in other pieces of legislation (e.g. the definitions relevant for data protection) and therefore no problem may arise in practice;

- Absence of cross referencing: No referencing is made to the Schengen Convention for 21 Member States. In this case, the conformity issue might not pose a problem in practice as the Schengen rules are in force in the Member States bounded by the Convention; and,
- Absence of minimum and or maximum levels of sanctions: Minimum and maximum thresholds appear to be missing in seven Member States despite the provision in Article 4 of the Directive.[12]

On a positive note, all Member States adopted at least one of the two additional measures foreseen by the Directive:

- 10 Member States adopted additional sanctions carriers [13]; and,
- 18 Member States used API data for law enforcement purposes (as allowed for by the last paragraph of Article 6.1)[14].

2.4.2 Analysis of the quality of implementation

Over half of the Member States had implemented API systems by May 2012 (i.e. 19 out of 30)[15]. Six Member States[16] planned to launch APIS by 2013 and one other[17] by 2015. Five countries do not currently have API systems in place and do not have any concrete plans to implement them in the near future.[18]

All implementing Member States use API for border management and the fight against irregular migration purposes, in line with the main aims of the Directive. As explained above, 18 Member States[19] have chosen to transpose the option of using API data also for law enforcement purposes; all of them are implementing API systems. Of these, nine Member States[20] make use of API data for law enforcement purposes. The scope of implementation of API systems varied: all Member States collected API from air carriers only three[21] also collect API from sea carriers. Some Member States[22] often collected API only from selected flights which had been assessed as 'at risk' of carrying irregular migrants and others implement API systems that collect API from all non-EU flights[23].

Authorities responsible for implementing national legislation and API systems generally included Border Management Authorities or Ministries of Interior and data protection authorities. While the former were generally responsible for ensuring compliance with API legislation and operating API systems, the latter were generally responsible for ensuring national authorities' compliance with data protection rules.

API systems have not been fully standardised across the EU / EEA and, subsequently, implementing countries place different requirements on carriers with regard to the mandatory data fields and the method of API data capture and transmission. API data were frequently

[11] More detail is provided in section 5.2.2.

[12] A detailed account of the countries is given in the full body of the report (see section 5.2)

[13] BE, CY, DK, EL, ES, IE, IT, NL, NO and the UK

[14] AT, BG, CY, CZ, EE, ES, FI, FR, DE, HU, IS, MT, LT, LU, LV, PT, RO and the UK

[15] AT, CH, CY, CZ, DE, DK, EE, HU, IE, IT, IS, LV, LT, LU, MT, NL, RO, ES, UK

[16] FI, FR, GR, PL, PT, SI

[17] SE

[18] BE, BG, NO, LI, SK

[19] AT, BG, CY, CZ, DE, EE, ES, FI, FR, HU, IS, MT, LT, LU, LV, PT, RO and the UK

[20] AT, CZ, EE, ES, FR, DE, HU, RO and the UK

[21] DK, ES, UK

[22] AT, CH, CZ, DE, HU, IT, NL, LV – DK and MT also only collect API from selected flights, but it is not clear whether this is based on risk assessment or not.

[23] CY, EE, IE, RO, ES, UK

captured by swiping machine-readable travel documents through 'SWIPE' reader technology; although, as air carriers have not always set up such technology in all third countries, some Member States[24] accept API data which have been typed-in manually. API data were transmitted through either a 'push' or 'pull' technique. The timing of capture[25] and the timing of transmission[26] also varied from country to country.

In all Member States API data were used by border guards to prepare for the clearance of passenger at the border. In most Member States[27] API were checked manually or automatically against 'watch lists' or specific national and European databases such as the Schengen Information System (SIS) and Visa Information System (VIS). In most Member States when API matches any entry on a watch list, an alert was sent to the border police at border crossing points and the corresponding passenger was targeted for examination on arrival.

In line with the Directive and existing EU legislation, API has to be deleted by carriers and authorities within 24 hours. However, Border authorities can retain them for longer for statistical[28], judicial[29] or law enforcement purposes[30]. At least one Member State[31] anonymised API data when retained in excess of 24 hours while many Member States restricted access to API data by making use of data security tools[32].

Finally, few implementing countries have implemented systematic monitoring of compliance of national API systems with data protection standards and API systems were rarely inspected by data protection authorities[33].

2.5 Results and impacts of the Directive

The results of the Directive have been assessed against five main evaluation criteria:

The relevance of the API Directive is assessed according to (1) the extent to which its objectives are pertinent to the needs, problems and issues to be addressed and (2) to the extent to which they are coherent with those of API systems in the Member States, national and EU related legislations.

[24] AT, CH, CZ, DE, DK, IC, HU, MT. RO

[25] i.e. whether capture takes place either at check-in or on boarding, following ticket inspection.

[26] i.e. whether transmission takes place immediately after check-in, after boarding, or after take-off.

[27] AT, CH, CZ, EE, FR, DE, HU, IS, IE, LV, LU, MT, NL, RO, ES, UK

[28] i.e. statistical analysis

[29] i.e. the prosecution of offences compromising security at the border

[30] i.e. retaining evidence against the offender for criminal/petty offences in judicial proceedings.

[31] NL

[32] e.g. encryption/decryption mechanisms and anonymisation. Member States have to anonymise or to delete data after 24 hours according to Article 6(1) of the Directive 2004/82/EC. Only if data are needed later for the purposes of exercising certain statutory functions (on the basis appropriate legal provision), they can be stored longer than 24 hours through . In the latter case a pseudonymisation can be useful. Otherwise data has to be deleted or anonymised. It is not legal to store pseudonymised data longer than 24 hours without a legal basis. See section 5.2.6.

[33] For a more detailed analysis of what the functions of the DPAs are in this regard, see section 6.7.

Relevance of the Directive to the needs, problems and issues to be addressed (1)

In terms of relevance of the Directive to the needs for intervention, 55% of the stakeholders viewed combating illegal immigration and 41% improving border control as the most important objectives. Member States competent authorities with a longstanding tradition of fighting against terrorism also identified law enforcement as a perceived need at the time of transposing the Directive.

For 28% of the Member State competent authorities the overriding reason for transposing and / or implementing the Directive was to comply with the Immigration and Asylum acquis as part of accession to the Schengen Area with no particular national needs, problems or issues identified a priori.

Coherence of the Directive's objectives with those of APIS, national legislation and related EU instruments (2)

The objectives outlined in related EU legislation, national legislation, as well as those driving the implementation of API systems, were considered compatible with those of the API Directive. However, in practice the provisions of the national implementing measures in some Member States might not have been coherent fully in line with the objectives of Data Protection legislation and with the Free Movement of Persons' acquis[34].

2.5.1 Effectiveness

The effectiveness of API systems is assessed in terms of (1) the extent to which systems contribute to the achievement of the objectives of the Directive, (2) the extent to which API systems are implemented effectively (3) the extent to which API systems are compliant with those of the Directive and (4) the extent to which API systems comply with data protection obligations.

Effectiveness in achieving the objectives (1)

Overall national stakeholders report that API systems have contributed to the achievement of the objectives they were set up to address. According to stakeholders, API systems have to some extent facilitated the improvement of border controls and contributed to the reduction of irregular migration. API systems were also considered as effective in improving law enforcement where this was recognised as an objective.

API systems are considered to have contributed to reducing irregular migration by improving risk-based profiling of international passengers; increasing the rate of detection of persons identified as irregular migrants.

API systems have been effective in improving border controls, primarily in helping border management authorities to better prepare for the control of specific passengers through advance screening of their API data. However, the effectiveness of API systems in improving border controls has been limited because the relative quality of API data submitted by carriers.

Finally, in the context of law enforcement, API systems have helped identifying persons posing security risks and other persons including victims of human trafficking and smugglers.

Implementation effectiveness (2)

Many Member States either implemented API systems in a recent past, or in early 2012 had yet to implement them. The most common obstacles to implementation included technological issues[35] (for 7 Member States)[36], lack of finances (4)[37], lack of political or

[34] For more information about these aspects, see Section 7.1.4.

[35] e.g. lack of compatibility between the information systems of authorities and those of carriers.

[36] BE, FI, GR, LT, NO, SI, SE

[37] BE, GR, LV, SK

stakeholder will (4)[38] and lack of appropriate legislative implementing rules (3)[39]. Carriers in general complied with API obligations and only a few Member States issued sanctions.

The extent to which API systems are compliant with the requirements of the Directive (3)

Overall the data collected and transmitted by carriers was mostly compliant with data requirements listed in the Directive, although some Member States requested additional data. The list of data provided by Article 3.2 of the Directive has indeed been interpreted by some Member States as not being exhaustive. Around a third of implementing Member States reported that on occasions they received faulty or incorrect API or that API had not been sent at all. The same proportion issued sanctions against carriers at least once over the period. API data was perceived to be useful by all implementing Member State competent authorities. Most Member States consistently processed API every time that it was received.

Mechanisms were in place to ensure that passengers were informed of API data being collected and redress procedures in all Member States; however it is difficult to assess the effectiveness of these systems without consulting passengers on a wide scale[40].

Effectiveness in complying with data protection legislation (4)

In relation to data protection, safeguards were built into all API systems to ensure data was secure and protected. Overall, stakeholders had not experienced any major problems in relation to data protection, including fundamental rights breaches. There had been very few complaints made to DPAs regarding use of API. However, it is not clear whether this is because data protection arrangements were working well, or because passengers were not fully aware of the use of API data. Moreover, the compliance of API systems with Data protection rules in Member States was not systematically monitored in most cases.

2.5.2 Efficiency

Efficiency is assessed in terms of (1) the cost efficiency of the API systems, (2) the cost to national competent authorities and (3) the implementation and compliance cost for carriers.

The overall efficiency of the Directive

From the perspective of competent authorities, API systems have had an impact at reasonable costs. However, it has not been possible to systematically qualify these judgements by outcome data so as to make direct comparison between costs and impacts. Although the overall efficiency with respect to outcomes of the API data collection is difficult to measure, conclusions can be made in some Member States:

- From 2010 to 2011, Austrian authorities have taken action against 0.4% of all international passengers whose API data had been collected;
- In 2011, Italian authorities have taken action against 0.7% of all international passengers whose API data had been collected;
- Over the past four years (2008-2011) in Germany, c. 7% of flights were identified as carrying at least one wanted person as a result of the API data checks; and,
- In the UK from 2005 to 2011, about 17,000 persons have been returned directly in relation to the monitoring of API and 27 facilitators have been arrested. In addition, 240 lost/stolen passports/documents have been seized.

Overall, the obstacles encountered in achieving the objectives of the Directive in a cost-efficient manner mainly related to the costs of implementation for national authorities and carriers. Moreover, the gradual implementation of API systems, partially through pilots, for which the full intended benefits have not yet been achieved, had made the measurement of efficiency difficult.

[38] BG, IE, LV, SI

[39] LV, PL, PT

[40] Surveying passengers was not possible within the limits of this study.

Cost of API systems to national competent authorities

The functioning of the Directive required border management authorities to invest in API systems. The cost of which varied depending on the objectives of the system implemented, its technical capabilities, the volume of API data processed and whether the system was dedicated to API data flows or part of a wider integrated border management systems.

The costs of API systems varied considerably between implementing Member States: from €9k per annum for a pilot in one airport authority to €4 million per annum for a highly advanced technological system. For an integrated border management system (such as e-Borders in the UK), in which the API capability is only one feature of the system, the costs of implementation were estimated at €175 million by the competent authority, with the cost of first year of operation representing approximately at €20 million.

Overall, API systems have not had a large impact on the relevant competent authority's operating budgets. In the majority of cases there had either been a small increase or no increase in the department's annual budget as a result of the implementation of API systems.

Cost of API data capture and transmission to air carriers

Overall, carriers consider that the Directive has not been cost efficient as it has not delivered tangible benefits in their favour. Implementing API systems diverted carriers from undertaking core business activities so as to deal with API data and brought costly changes to customer practices relating to collection and transmission of API data.

The API Directive-related compliance costs for carriers ranged from less than €0.5 million for smaller air carriers to over €2 million on average per carrier per annum for major air carriers after the set-up costs had been absorbed[41]. The difference being mainly due to the number of international routes each carrier operated and the sophistication of the API systems implemented.

2.5.3 Impact

The implementation of the Directive generated (1) impact on border control and border management (2) Impacts with regard to fighting irregular migration and law enforcement (3) Impact on carriers (4) impact on airport authorities and passengers (4) impact in third countries as well as unintended impacts (5).

Impact on border control and border management

Overall, implementation of the Directive has improved border control procedures and made border checks faster. As a consequence of the API systems, the border management authorities have become better prepared for undertaking border control activities. Overall, the implementation of API has helped to improve border controls, as API data rendered advance screening of international passengers possible, providing additional time and an increased ability to target in advance "at risk" passengers and routes.

Impact on combating illegal immigration and impact on law enforcement

Implementing API systems have had the most impact in relation to improved management of staff used to combat illegal immigration and improved targeting of suspect illegal immigrants. API also had an impact on improving the knowledge of competent authorities on the main migration routes through which irregular migrants travel and to an extent had increased refusal of entry to illegal immigrants.

The impact of API systems on law enforcement was perceived as secondary to those on border management and illegal immigration. However, API systems have had a clear impact on improving security at the border and to some extent on the arrest and prosecution of

[41] This is based on information provided by eight carriers consulted in this study, six of which provided a response to the online industry survey.

criminals. Anecdotal evidence from selected Member States with respect to the overall use of API data (covering any purpose including law enforcement[42]) shows that:

- from 2010 to 2011 Austrian authorities recorded 12,332 cases where API data had been used by the border management authorities to take action against international passengers;
- in 2011 Italian authorities recorded 85,222 cases where API data had been used by the border management authorities to take action against international passengers.
- from 2008 to 2011 2,322 persons have been refused entry at the UK border as a result of API data used by the border control authorities.

Impact on carriers

The implementation of the Directive impacted carriers in three ways: (1) financial impacts of capturing and transmitting API data, (2) financial impact of non-compliance (3) and changes to business processes.

Air carriers perceived the implementation of the Directive as over-burdensome leading to costly implementation with little or no direct business benefits. As some carriers could not use their legacy systems or where impacted by several but different national API data requirements the latter resulted in additional costs of upgrade of the existing systems.

With regard to non-compliance over 180 sanctions representing €1.7 million worth of sanctions were paid by carriers to at least six Member States over the evaluation period. These were imposed on the grounds of faulty or incorrect data or a late transmission of data in six Member States. However, this was not necessarily a reflection of carriers' compliance but the ability and willingness of authorities to impose sanctions.

Generally, the carriers had a negative perception of the impacts of API. Implementing API systems had diverted carriers from undertaking core business activities to dealing with API data and brought costly changes to customer practice relating to collection and transmission of additional information. The changes were seen not to have brought improvements in the timeliness of flights or general carrier security.

Impact on passengers and airport authorities

Impacts on passengers and airport authorities were not particularly strong, and there was considerable variation in the views of competent authorities and carriers on this matter.

From the perspective of competent authorities the results of the implementation of the Directive are twofold: in made air traffic more secure and passengers were cleared faster at the border. Some competent authorities considered that airport operations functioned more effectively, and that overall passenger convenience had improved. These views were not supported by a majority of carriers who had not noticed significant improvements in these areas. Lastly, the impacts on the airport of departure may have been slightly negative because of additional processing time required by API data capture but these may have been partially offset by reduced queuing time at the airport of destination.

Impacts on third countries and impacts on international relations

The impact of the Directive on third countries and on international relations has been relatively limited. There has been little impact on third countries apart from that API data had been requested from third country carriers and changes in practices of third country airport operators have taken place. Implementing API systems has not contributed to improving relations between the EU/EEA and third countries though it had not had a negative impact either. Anecdotal evidence showed some reluctance of third countries to have passenger data to be collected from their citizens.

Unintended impacts

[42] The data available does not allow to distinguish clearly among the various purposes for which API is used, especially in the case of law enforcement.

Unintended impacts tend to be specific to national circumstances and to the context in which API systems were implemented:

- While most Member States have transposed the API Directive into their national legislations, a minority of Member States did not have the technical capacity or sufficient resources to process API data;
- Additional requirements of Member States and their deviation from internationally recognised standards in the field meant that carriers had to bear unnecessary additional cost of compliance or had to spend time collaborating with Member States to negotiate a suitable solution;
- In some Member States, API data have also on occasion been used for purposes beyond border control, migration management or law enforcement. For example, in the UK, at the time of the swine flu outbreak, the national air carrier had to keep API data on passengers for longer so that authorities could keep a record of persons travelling at that time. The benefits were to monitor the epidemic and take appropriate action.
- API data were used for situational awareness and profiling: statistical analyses enabled Member State authorities to identify risk factors (i.e. citizenship of passengers, country of origin, flight routes, etc.)
- Synergies in developing and implementing API systems: although the Directive did not contain incentives for Member States to jointly develop technological solution or systems, some Member States took the opportunity to build on already established systems[43].

2.5.4 Added value

Added value concerns the extent to which EU action has brought added value in comparison to similar Member State level actions and initiatives. It is assessed taking account of various stakeholder perspectives:

While some Member States and most air carriers questioned the added value of the Directive, the majority of the national competent authorities considered that the Directive had a specific identifiable added value with respect to adoption of the API systems and the increased capacity to process information faster in order to identify illegal immigrants and suspect criminals.

The Directive brought added value to the national authorities in charge of border control and law enforcement in accelerating the timeliness of the adoption of API systems technology and related practices. At the time of the adoption of the Directive a few Member States had planned to implement API systems[44]. Although it is not possible to assess with certainty whether or not Member States would never have adopted such systems if the EU Directive was not adopted, its introduction certainly sped up the adoption of related technology and new border control management and law enforcement practices.

The main concerns were that patchwork implementation reduced the added value of the Directive and that in some Member States there was not a strong business case to support the implementation of API systems, particularly when air borders were already strongly regulated.

From the carriers' perspective, the collection and transmission of API data did not provide any added value as there was no commercial need or use for such information, and it did not allow stopping suspect persons from boarding the plane, hence not specifically improving carrier security (e.g. in-flight security).

[43] For instance, Switzerland adopted many parts of the German API system.

[44] i.e. DK, ES, UK

2.5.5 Unintended benefits and drawbacks to the implementation of the Directive

From the airline industry's perspective the API Directive did not bring benefits for air carriers. The main reason being that the Directive did not specify standards or implementation guidelines which would have enabled more joined up implementation at EU / EEA level. According to industry stakeholders, this resulted in a patchwork implementation in each Member State where requirements and obligations imposed on air carriers deviated from internationally established best practices. The end result was that the various national requirements had a negative impact on air carriers flying routes to Europe.

On the positive side, the main unintended benefits that had materialised as a result of the adoption of the API systems included:

- Investment in systems and infrastructure to process API data flows in a technologically advanced manner;
- Adoption of new Border control practices;
- Widespread adoption of enhanced border control technologies may have created a level playing field for such systems, bringing the costs systems down and helping further the implementation of such systems and processes.

2.5.6 Main conclusions

The main conclusions are categorised along the following themes:

- Quality of the transposition of the Directive into the national legal system:
  - The vast majority of Member States' legislation is not in full conformity with the Directive. However, formal issues of conformity do not always correspond to problems in the overall national legal systems or in practice;
  - The main issues of non-conformity relate to data protection legislation with regard to the length of retention of API data by authorities and carriers; late transposition, and absence of minimum and/ or maximum levels of sanctions.
  - There have been some concerns among Member States that API data is being collected on intra-EU flights. This might also mean that obstacles have emerged precluding EU citizens and their family members to fully enjoy their right to move and reside freely
    The study evidenced various interpretations by Member States of the use of API data for "law enforcement purposes" and it is not clear if all uses are in line with the objectives of the Directive.

- Quality of the implementation of API systems:
  - This study has shown that nineteen Member States currently implement API systems. In addition, six Member States planned to launch API systems by 2013 and one other by 2015. A remainder of five countries do not currently have API systems in place and do not have any concrete plans to implement them in the near future.
  - API systems' technical and operational capabilities and their scope of application vary: for instance all implementing Member States use API data for border management and the fight against irregular migration purposes while nine of them also make use API data for law enforcement purposes. Moreover, API obligations are imposed on air carriers in all implementing Member States while only three of those collect API data from sea carriers and none from land carriers.
  - In all Member States API data were used by border guards to prepare for the clearance of passenger at the border. In most Member States API data was checked against 'watch lists' or specific national and European databases (i.e. VIS, SIS);
  - Few implementing countries have implemented systematic monitoring of compliance of national API systems with data protection standards
- Results of the Directive
  - With regard to its relevance, the Directive was perceived as aligned to the objectives of combatting illegal immigration and improving border control. However, in practice

the provisions of the national implementing measures in some Member States might not have been coherent or fully in line with the objectives of the Data Protection legislation and with those of the Free Movement of Persons' acquis;
- With regard to its effectiveness, API systems have contributed to the achievement of combatting illegal immigration and improving border control. For instance, the implementation of API systems has helped to improve border controls, as data has been received in advance, providing additional preparatory time and an ability to target in advance passengers who are subject to an 'alert'.
- API systems were also considered as effective in improving law enforcement where this was recognised as an objective: the use of API data enhanced internal security and public order in those specific Member States.
- With regard to its other impacts, Directive had a relatively limited effect on third countries (e.g. airport operators, carriers, etc.) or passengers.
- With regard to efficiency, national authorities perceived that API systems have had an impact at a reasonable cost; whereas from the carriers' perspective this has not been the case as they were unable to realise benefits from necessary investments to meet their compliance requirements.
- With regard to added value, the Directive has brought added value to the national competent authorities in charge of border control and law enforcement in several ways: primarily through accelerating the adoption of API systems, by increasing the capacity to process information faster in order to identify illegal immigrants and suspect criminals and through establishing more innovative border control practices. However, the patchwork implementation of API systems across the EU may have limited the added value of the functioning of the Directive, mostly in relation to the range of benefits to be derived from API systems.

Overall, the adoption of the Directive by Member States had a positive impact on border control practices and on the better identification of irregular migrants and or suspected persons for national authorities. The costs of implementation were seen as high by most stakeholders, especially by carriers. However, it may be too premature to conclude on the cost-effectiveness of the Directive in view of the early stage of its implementation. National authorities nonetheless recognised the potential of API systems and related technologies in the fields of border control, fight against irregular migration and fight against serious crime.

2.5.7 Main recommendations

The study evidenced potential issues related to:
1. The quality of transposition and interpretation of the provisions of the Directive by Member States;
2. The functioning of the Directive and implementation of API systems in the Member States; and,
3. Monitoring and evaluation mechanisms and arrangements

The following recommendations are meant to address the above-mentioned potential issues:
1. To address potential issues related to the transposition and interpretation of the provisions of the Directive the Commission may consider:
   - Contacting Member States and taking appropriate action to ensure they correctly transpose the following provisions:
     - the obligations of Member States with regard to the legislation on freedom of movement of persons;
     - the time limitation for the retention of API data by both the carriers and the authorities; and,
     - minimum and maximum amounts of sanctions foreseen in Article 4 of the Directive.
   - Laying down guidelines and recommendations on the matters below:
     - Use of data for "law enforcement" purposes, including its definition in this context. This might include but might not be limited to the enforcement of border security, internal security, custom and national security related legislations;

- The maximum set of API data to be transmitted by carriers in line with ICAO/IATA/WCO guidelines;
- Application of the Directive with regard to EU nationals and intra-EU flights.
- How to comply with the data protection provisions of the Directive 2004/82. This would be particularly pertinent with respect to the data retention period for the purposes of law enforcement, access restrictions to API data by authorised officials, and the minimum safeguards required for data transmission and data retention. The prime target audience for these recommendations would be the national authorities and the carriers. One of the expected impacts would be Data Protection Authorities to inspect API systems to verify their compliance with data protection laws on the basis of a clear guidance issued by the national legislators.

2. To address potential issues related to the functioning of the Directive and implementation of API systems in the Member States the Commission may consider:
   - Adopting guidelines based on the internationally recognised good practices in the area (e.g. PADIS; UN/EDIFACT; and « ICAO machine readable travel document formats »);
   - In the absence of internationally recognised good practices, it is recommended that the Commission identifies ways in which Member States could remedy to sub-optimal implementation of API systems:
     - The Frontex Advance Information Working Group could advise on ways to remedy issues occurring at each stage of the API data treatment and corresponding standards: data capture (effective and compliant ways of capturing API data and consistent data field requirements across systems), data transmission (best methods to transmit data manually, semi-automatically and automatically in a secure and efficient manner) and data matching (data aggregation, data cleaning and data matching to EU and national databases). In addition, this group could design frameworks for security practices (e.g. for the secure transmission, encryption, access, retention and deletion of API data) and for compliance regimes (i.e. processes to incentivise carriers compliance and common sanction regimes and guidelines)
     - Continuing to regularly liaise with Working Groups from AEA, ICAO, IATA and WCO to keep abreast of the latest developments, standards and good practices on advance passenger information so as to incorporate good practices in the follow up of the recommendations and encourage other programmes or initiatives. Supporting the exchange of good practices between competent authorities to maximise the benefits from the implementation of API systems. The themes best suited to exchanging practices include (1) Benefits of and approaches with regard to risk analysis and risk profiling (2) Benefits of and methods for extending of API systems to other carriers (i.e. maritime and land transport mode) (3) Efficient mechanisms used for API data capture, transmission and reception, data processing capability, data matching and methods for realising the full benefits of API systems (4) Efficient integration of API systems with existing databases and with physical checks at the border, in order – for example – to identify migrants who destroy documents mid-flight and/or 'switch' identities (e.g. by including biometrics).
     - Singlehandedly or jointly procuring a set of studies on (1) the extent to which existing capabilities of each port and each carrier allows for the cost-efficient, timely, automated and secure capture and transmission of API data; (2) the set of optimal time windows for data transmission, which maximise security, quality and accuracy of the data taking account of carrier and third country circumstances; and (3) a cost-benefit analysis on API systems and specific practices to maximise the benefits from the implementation of API systems.
     - Supporting the exchange of personnel between competent authorities as well as capacity building activities such as training, technical assistance, etc. This will help building a community of practice with regard to API systems in the EU.

- Encouraging the joint development or technological innovation for API systems, potentially to help reduce the costs of implementation and also to increase the API systems' coherence in the EU/Schengen area and application of common standards. This could also have the benefit to spur innovation if implemented through research grants to consortia mixing industrial and public sector partners.

3. To address potential issues related to monitoring and evaluation mechanisms and arrangements, the Commission may consider:
   - Laying down recommendations on key indicators and statistics to be gathered to guarantee the adequate monitoring of the Directive in view its future evaluation or revision. The benefits would be to better measure the overall efficiency of the API in the future in order to also better understand the benefits of different types of API systems and whether they justify the level of investments made, both from the perspective of the carriers and the national competent authorities.

3 Overview of the study methodology

This section of the report provides an overview of the study methodology and summarises the work which has been undertaken throughout the course of the assignment.

3.1 Main evaluation themes and sub-themes

This section sets out the evaluation questions that are being assessed as part of this assignment. Table 3.1 lists the main evaluation criteria that are used for assessing the compliance and the quality of the transposition of the Directive, whereas Table 3.2 indicates the main evaluation criteria and corresponding questions for assessing the functioning of the Directive. The theme column in the tables denotes the analysis requirement stated in the Terms of Reference[45].

[45] For example, procedural issues (1,2) means that the corresponding evaluation question relates to the analysis area of 'procedural issues' and more specifically bullet points 1 and 2 under this heading in the ToR.

Table 3.1 Main evaluation criteria for assessing the compliance and the quality of the transposition of the Directive

Evaluation criteria	Evaluation question	Theme
Quality of the transposition	How timely was the transposition of the directive into national legislations? Has the deadline for transposition of the directive into the national legal framework been met?	General/legal issues (1,5,6)
	Have all the provisions of the Directive been transposed and implemented by national measures? If not which ones?	General/legal issues (1,5,6)
	Are there any national measures which go beyond the obligations as prescribed in the Directive? If so which ones?	General/legal issues (1,5,6)
	What is the extent to which the national measures conform to the article of the API Directive?[46]	General/legal issues (1,5,6)
Quality of the implementation	What are the main processes through which the API data is transmitted? Are national authorities granted automated access to API data?	Procedural issues (4,5 –means of access)
	What is the organisation of the respective national authorities responsible for implementation and application of the Directive? What is the remit and powers of the national authorities and those of their parent authorities?	Procedural issues (4,5 –contact points and whom information handed)
	What are the main technology solutions for data transfer? What are the pros and cons of implementing the API regarding the infrastructure needed to transmit information, taking into account the requirements of personal data protection?	Procedural issues (5) General/legal issues (4)
	What is the overarching governance framework for ensuring compliance with related Directives (i.e. freedom of movement and data protection)	*Procedural issues (other)*
	Are there any problems arising from the implementation of Directive in terms of Fundamental Rights (i.e. right to freedom of movement, data protection, etc.)[47]	*Procedural issues (other)*
	What criteria has been used to determine: (i) whether and to what extent checks could be automated or whether human intervention is required; (ii) whether solely electronic online information can be submitted or alternative solutions exist	Procedural issues (1,2)
	What type of transportation is currently covered?	General/legal issues (6)
	Where does the API system fit within the integrated border management system?	*Procedural issues (other)*
	What are the main databases against which API is being checked? And the procedures to check against these (e.g. hit/no hit; automatic access?)	Personal data protection issues (2)
	How are international passengers informed of the use of their personal data? What type of information is provided to him?	Personal data protection issues (5)

[46] Removed from the question: and other related Directive?

[47] In the proposal this was under transposition, but it was judged to be better placed under the implementation section.

Table 3.2 Main evaluation criteria and corresponding questions for assessing the functioning of the Directive

Evaluation criteria	Evaluation question	Theme
Relevance and coherence of the Directive: To what extent the objectives of the Directive are pertinent to the needs, problems and issues to be addressed? To what extent its objectives coherent with those of API systems in the Member States?	To what extent the purposes of the API systems created match the objectives of the Directive? What criteria have been used to determine the carriers for which API should be applicable?	General/legal issues (1, 5)
	To what extent the intended benefits of the national API systems respond to the needs, problems and issues as identified at national level in the field of irregular migration and internal security? Do they match those of the Directive?	General/legal issues (2)
	To what extent the obligations of the Directive are in line with other obligations of related Directives (i.e. Data Protection Directive)? Are there some issues in terms of coherence and if so what are they (i.e. political, practical issues)?	Personal data protection (3)
Effectiveness : To what extent has the Directive achieved its stated objectives?	To what extent the API Directive has contributed to improving border controls in Member States and in the EU?	Authority/stakeholder related issues (1)
	To what extent the API Directive has contributed to combating irregular migration in Member States and in the EU?	Impact / results
	To what extent the API data collected and transmitted by carriers compliant with the data requirements listed in the Directive?	Personal data protection (1,3)
	To what extent the API data transmitted to national authorities is used, and for which purposes has it been used?	Impact / results
	To what extent the management of API data (i.e. retention and protection) by national authorities and carriers is compliant with the obligations and safeguards for data protection as listed in the API Directive?	Personal data protection (1, 3)
	Are appropriate measures in place to inform the traveller of the collection of their data with respect to: ▪ How the traveller is informed on the use of their data ▪ Information provided to the traveller (e.g. purpose for which data collected, type of data collected, retention period, right of access to data) ▪ Information on right of access to their data and correction and deletion of such data	Personal data protection (4,5,6)
	Have there been instances of data protection breaches? What are the disadvantages / problems that API might pose in light of international relations, fundamental rights/civil liberties, and practically and politically in general?	General/legal issues (3)
	What is the amount of financial sanctions imposed on carriers? What other sanctions have been imposed?	Authority/stakeholder related issues (6)

Efficiency: To what extent are resources being efficiently used in achieving the Directives intended impact?	What have been the costs related to the practical implementation of API systems for Member States carriers?	Costs (1)
	What are the operating costs of running API systems for Member State authorities and carriers?	Costs (1)
	What has been the number of passenger affected by the API Directive since the implementation of the Directive?	Costs (2)
	How soon after the transposition of the Directive the API systems in Member State were operational (time-frame for implementation)?	Costs (3)
Impacts of the Directive and added value	What have been the main impacts of the Directive in third countries (i.e. policy impacts, impacts on airport and harbour operators)?	Authority/stakeholder related issues (4)
	What have been the main impacts of the Directive on border control (i.e. border control procedures, technological innovation, number of irregular migrants apprehended and number of refused travellers)	Authority/stakeholder related issues (1,7)
	What have been the main impacts of the Directive on law enforcement authorities (i.e. extent data used for law enforcement purposes, in how many cases, for which specific purpose and by which authorities)	Authority/stakeholder related issues (5)
	What have been the main impacts on carriers and their industries, including for cruise line companies and air/rail traffic in Member States where API is implemented to this effect? (i.e. operations, costs)	Authority/stakeholder related issues (1,2)
	Have best practices been identified (i.e. process automation, submission of information, transmission of information, information management, cooperation mechanism, technological advances)?	Implementation and best practices
	What have been the main impacts on passengers (e.g. convenience, travel experience and wellbeing)?	Impact / results
	What has been the added value of the Directive?	Added value
	Have there been some unintended benefits and drawbacks to the implementation of the Directive (i.e. spill over effects, etc.)	Unintended impacts

3.2 Data collection

This section provides an overview of the data collection activities undertaken as part of this study. For a detailed overview of the method, the inception report should be consulted.

3.2.1 Mapping of national legislation and API systems (steps 1.1 to 1.4)

Two mapping exercises have been undertaken for 30 examined EU Member States[48]:

(i) **Legislative mapping (transposition studies)** - mapping of national transposing measures of the API Directive, and

(ii) **API system mapping** – mapping of the implementation of API systems in practice

The transposition studies aimed at mapping the existing national legislation transposing each provision of the API Directive and highlighted potential conformity problems (i.e. cases where the transposition is not in line with the requirements listed in the Directive). In addition, the mapping of the API system focused on the implementation of the API Directive in practice. Based on findings and the stakeholder interviews, it aimed at providing a thorough overview of the functioning of the national API systems.

The assessment of **the transposition of the API Directive** has been relevant to all EU Member States The assessment of **the functioning of the API system** has been relevant only to 19 Member States which currently have an API system in place[49]. With respect to those 19 countries implementing API, the assessment of the implementation of the API includes overview of the functioning of the API directive; remit and activities of national stakeholders as well as operation and characteristics of the API system. With respect to non-implementing countries, an overview of the ***intended*** functioning of the API is provided, including a description of the intended functioning of the API Directive as well as the remit of key stakeholders involved in the implementation of the Directive.

The assessment of the quality of transposition and the implementation of the API system has been competed with respect to all EU Member States. The results of the assessment are provided in sections 5 and 6 of this report.

3.2.2 Stakeholder interviews

Stakeholder interviews were undertaken in the data collection phase of the evaluation. The main national stakeholders contacted were Border Management Authorities, Ministries of Interior and Data Protection Authorities. In some Member States interviews with other relevant national authorities have been carried out, such as Permanent Representation to the EU and Ministry of Transport. In addition, interviews with a sample of national carriers were undertaken.

In regard to the countries currently not implementing API systems, only the border management authorities were contacted, while in regard to the implementing countries, further interviews with national stakeholders were undertaken. This included interviews with Ministries of Interior, Data Protection Authorities, Ministry of Transport and Permanent Representation of the Member State to the EU.

Overall, interviews were conducted in 30 Member States. No interviews were planned in Lichtenstein as the country does not have an airport and does not implement or plan to implement an API system in practice. In addition, in order to obtain a complete picture of the implementation and functioning of the API Directive, representatives from international organisations have been interviewed. Interviews were carried out with representatives from SITA, IATA and IBM.

[48] Liechtenstein would have had to transpose the Directive but it does not have an airport. Therefore, Lichtenstein has not been considered in the analysis of the transposition of the Directive.

[49] AT, CY, CZ, DK, EE, FR, DE, HU, IT, LV, LU, MT, NL, RO, SL, ES, UK, CH and IS

In total 72 interviews have been carried out as part of this study. 68 of these related to consultations at national and international level, whereas three interviews were carried out with the Commission officials from DG Home and DG Justice (Unit C2: Union citizenship and Free movement and Unit C3: Data protection) as part of the inception phase of the study. Frontex was also interviewed in the inception phase of the study.

Table 3.3 below provides an overview of the number and type of stakeholders interviewed at national and international level. Figure 3.1 depicts the share of responses per stakeholder group and **Error! Reference source not found.** specifies the types of stakeholders interviewed in each Member State.

Table 3.3 Overview of the number and type of stakeholders interviewed

Stakeholder	Number of undertaken interviews
Border Management Authorities	34 in 27 Member States
Ministries of Interior	7 in 7 Member States
Data Protection Authorities	12 in 12 Member States
Other national authorities	1 interview (Permanent Representation of Hungary to the EU) and 1 interview with Transport Ministry in France
Air Carriers	9 interviews with 6 air carriers
International organisations	4 interviews in 3 organisations IATA, IBM and SITA
Total number of interviews	**68 interviews**

Figure 3.1 Proportion of interviews undertaken per stakeholder

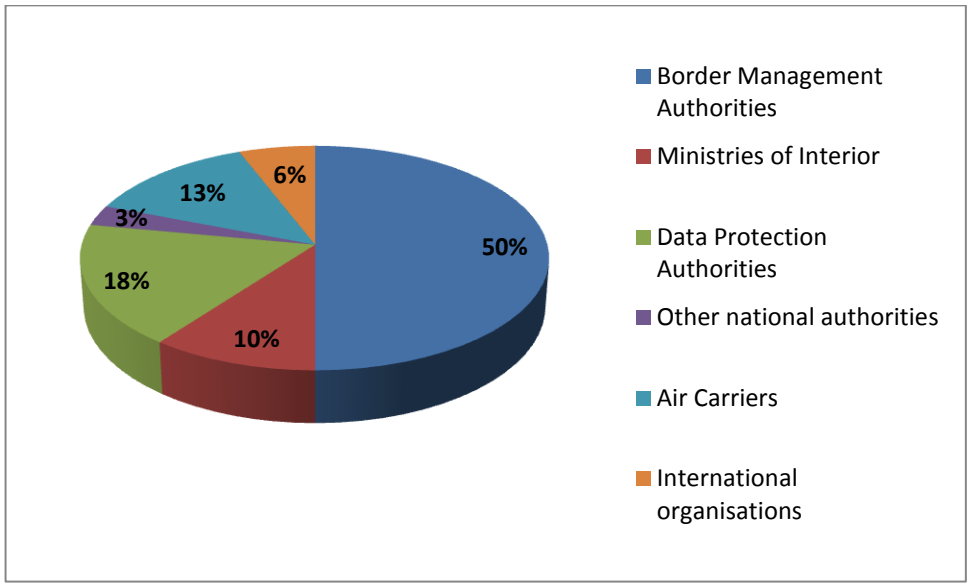


Table 3.4 Stakeholders consulted through telephone interviews in the Member States

Member State	Border Management Authorities	Ministries of Interior	Data Protection Authorities	Other national authorities	National carriers
AT		√ Section II/3 Foreign Police, Border Control, Visa, Border Control Matters, Schengen	√ Deputy Head of Office, Data Protection Commission		
BE	√ Head of Department, Airport Police				
BG	√ Head of unit "Border control activity", Border Police				
CY	√ (2 interviews) Cyprus Police 1)Research and Development Department 2)Aliens and Immigration Service				
CZ	√ Police of the Czech Republic – Directorate of Alien Police Service	√ Interior Ministry – Department for Asylum and Migration Policy	√ Legislation and Foreign Relations Department, Office for Personal Data Protection		
DK	√ Danish National Police, Aliens Department		√ State Secretariat of Security. Subdirectorate General of Communication Systems for State Security		
EE	√ Border Security Bureau, Border Guard Department, Police and Border Guard Board	√ Migration and Border Policy department, Ministry of Interior	√ Director – General, Data Protection Inspectorate		√ Estonian Air, Security manager
FI	√ Border Authority				
FR	√ Head of Border Police	√ Ministry of interior, Unit of Freedoms	√ Legal Affairs Unit- Police Justice Department of the CNIL	√ Transport Ministry	√ (2 interviews) Air France
DE	√ Department 2 National Security, Unit 22 Border Police tasks, Federal Police Headquarters		√ Unit V Police, Secret Service, Criminal Law, European and International Cooperation in the fields of Police and Justice, Federal Commissioner for Data Protection		√ (2 interviews) Lufthansa

Member State	Border Management Authorities	Ministries of Interior	Data Protection Authorities	Other national authorities	National carriers
			and Freedom of Information (BfDI)		
EL			√ Head of EU Section of the Greek Police, Police Head Quarters, Ministry of the Interior		
HU	√ National Police Headquarters (ORFK)		√ International Affairs and Public Relations, National Authority for Data Protection and Freedom of Information	√ Permanent Representation of Hungary, Ministry of Interior, Ministry of National Development, Airport's Police Division	
IE	√ Principal Officer, Border Management Unit, Department of Justice and Equality				
IT	√ Head of 1St. Division in the Border Police		√ Service for European and International relations, Data Protection Authority		
LV	√ (4 interviews) Border control and immigration control service				√ Air Baltic
LT	√ International Cooperation Division, Border Control Organisation Board State Border Guard Service under the Ministry of the Interior				
LU	√ (2 interviews) the Central Unit of the Police at the Airport; Head of international matters. Grand-Ducal Police		√ President, National Commission for the Protection of Data		
MT	√ Malta Police, Immigration Section				
NL	√ Project leader API, Programme modernisation border management,	√ Policy and Legislation Unit, Program Directorate			

Member State	Border Management Authorities	Ministries of Interior	Data Protection Authorities	Other national authorities	National carriers
	Royal Military Police (KMar)	Identity Management and Immigration, Ministry of the Interior and Kingdom Relations			
PL	√ (3 interviews) Border Guard's Headquarter				
PT	√ Head of the Air Borders Core, Aliens and Border Service				
RO	√ Border Police				
SL	√ Police, Sector of Border Police , Ministry of Interior				
SK	√ Office of Border and Foreigners Police, Presidium of the Police Corps				
SE	√ National Police Board				
ES	√ Police General Unit for Borders and Foreigners				√ (2 interviews) Iberia
UK	√ Deputy Director e-Borders programme, UK Home Office		√ Information Commission's Office		√ British Airways
CH	√ Section: border, Federal Office for Migration		√ Swiss Federal Data Protection and Information Commissioner		
LI	***No interviews undertaken in Lichtenstein***				
NO		√ Ministry of Justice and Public Security			
IS	√ Border Authority	√ Ministry of the Interior			

3.2.3 Collection of cost data

The national stakeholders from countries, which are currently implementing the API system, were also requested to complete an Excel spread sheet collecting cost data. Eight Member States have provided the data.[50] The cost data sheets were aimed at collecting information on cost impacts of setting up, upgrading and/or operating national API systems. Full analysis of these results is included in Section 7 this Draft Final Report.

3.2.4 Online survey (Step 1.5)

Two online surveys were launched to supplement the stakeholder interviews and gather additional information. These were directed to national competent authorities and air carriers. The purpose of the survey was to gather information regarding the implementation and functioning of the obligation of carriers to communicate passenger data. The survey covered the following areas:

- Implementation of the system to process and use API ('API System');
- Efficiency and effectiveness of the API system;
- Impact of the API system; and
- Added value of the API system and best practices.

The national competent authorities (border management authorities, the border police, Ministry of Interior) in all EU Member States were invited to participate in the survey. The most relevant authority from each Member State was invited to provide a response. The survey was distributed via email invitation on 14th of May. Two reminders were sent on 23 of May and 8 of June to encourage participation

The final deadline for survey completion was 15 June 2012. By 15 June, 22 responses from 31 Member States were received, corresponding to a 68 per cent response rate.

A separate online industry survey was directed to air carriers. 21 airlines were selected, one carrier from each Member State implementing API, apart from Germany and UK where more than one carrier was included in the sample.

The survey was launched on 18 May 2012. It was distributed through the Association of European Airlines (AEA) and directed to the members of the API/PNR Working Group. The final deadline was set at 20 June 2012. The deadline was extended twice to encourage greater response rate. In line with this, reminders were sent twice on 18 May and 15 June to air carriers to encourage participation

Six responses were received from the selected airlines[51], representing 28 per cent overall response rate, but covering almost a third (31%) of all Member States implementing API.

The results of the online survey are included as part of the analysis in Sections 6 and 7 of this report.

3.2.5 Expert workshop (step 2.6)

The expert workshop was held on 11 June 2012 organised to discuss main issues identified with respect to functioning of the API systems, the proposed best practices and recommendations for the study. The workshop aimed to validate and discuss the main issues associated with the functioning of the API Directive and the implementation of API systems as well as to consider current good practices and identify potential further good practices amongst current API systems. Participants in the workshop included members of the project team from ICF GHK and Milieu and representatives from the relevant Directorate-Generals of the Commission and FRONTEX.

[50] AT, CH, DE, ES, IT, IS, RO and UK

[51] Czech Airlines j.s.c., Swiss International Air Lines Ltd, Air France, SAS, Brussels Airlines and Lufthansa

3.3 Data analysis

This section outlines the analysis activities that have been undertaken as part of the evaluation. The analysis has included thorough assessments of:

- The quality of transposition of the API Directive in all Member States
- The quality of implementation of the API Directive in those Member States implementing API and an analysis of reasons for non-implementation in those not currently implementing the Directive
- The results of the Directive, as well as the impacts (costs and benefits) of collection and transmission of API to the industry and border control authorities in Member States implementing API

These analyses are explained in the subsections below.

3.3.1 Analysis of the quality of the transposition (step 2.1)

The analysis of quality of transposition has focussed on the overall assessment of the transposition in the Member States of Articles 3, 4, 5, 6 and 7 of the Directive. The analysis has consisted of two main assessments: completeness and accuracy of the transposition. As indicated in the data collection section, the analysis is included in Section 5 of this report.

3.3.2 Analysis of the quality of implementation (step 2.2)

The purpose of the analysis has been to provide a detailed assessment of the implementation activities in the Member States. The analysis is presented in Section 6 of this report which provides an overview of the different types of API systems implemented as well as the remit and activities of stakeholders. The section also includes an analysis of the overall API systems as well as assesses problems with the implementation and reason why certain Member States have not implemented the relevant system to-date.

3.3.3 Analysis of the result s and impacts of the API Directive (step 2.3)

The method for assessing the results and impacts of the Directive follows the principles as set in the Inception report. The analysis of results and impacts has been organised according to the evaluation criteria (Relevance, Effectiveness, Efficiency, Impact and Added Value) taking into account of the evaluation questions for the study. The analysis includes an overview of the results (from uses of API) as well as the impacts of API (costs and benefits).

The results and impacts of API Directive are presented in Section 7 of the report.

4 Overview of the Directive

This section gives a brief overview of the Directive, in particular by describing its origins, objectives and purposes, elaborating on its intended results and impacts foreseen in the Directive and finally, presenting the intervention logic of the Directive's functioning.

4.1 Aims and objectives of the Directive

The Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (known as the API Directive) was adopted following an Initiative of Spain. The obligations provided for in the Directive are complementary to those laid down by Article 26 of the Convention implementing the Schengen Agreement, as supplemented by Council Directive 2001/51/EC, concerning the obligation of carriers to return third-country nationals who are refused entry by the Member State of destination. The Directive is a development of the Schengen *acquis* and, in this context, Lichtenstein, Switzerland, Iceland and Norway are bound by it.

The Directive has two aims, namely it aims at improving border controls and combating illegal immigration (Article 1). In order to achieve these aims, the Directive requires the Member States to establish an obligation for air carriers to communicate certain information concerning their passengers travelling to a European Union border crossing point by the check-in of their passengers (Article 3(1)).The information the carriers are obliged to transmit include: the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport and the initial point of embarkation (Article 3(2)). This information is supplied, at the request of the authorities responsible for carrying out checks on persons at the external borders of the EU, to improve border control and to combat illegal immigration more effectively. In principle carriers should transmit the information electronically to the authorities carrying out border checks at the authorised border checking point through which the passengers enter into the EU. However, in case of failure, the Directive also allows transmitting data by any other appropriate means (Article 6(1)). As a general rule, these data should be saved in temporary file and are to be deleted by the authorities within 24 hours after the transmission unless specific conditions apply. Carriers are also obliged to delete personal data within 24 hours of the arrival of the means of transportation (Article 6(1)). They are obliged to inform passengers about the processing of its data in accordance with the national law and subject to data protection provisions under Directive 95/46/EC (Art. 6(2)). Following this Directive, they are also obliged to inform the passengers about the right to access to and to rectify the data concerning them.

Should carriers, as a result of fault, transmit incomplete/false data, or fail to transmit data, Member States must adopt dissuasive, effective and proportionate sanctions. The minimum amount of sanction cannot be less than 3,000 EUR and the maximum should be at least 5,000 EUR. Carriers may appeal against measures imposed by the Member States. Member States need to guarantee that carriers can make use of their right of appeal and have effective rights of defence (Article 5).

The Directive foresees also a number of additional measures that the Member States can decide to apply or not. Member States are allowed to impose other types of sanctions (e.g. seizure, immobilisation) in case carriers seriously infringe their obligations arising from the Directive (Article 4) and the Directive leaves the possibility to apply its rules also to non-air carriers. To some extent and under certain conditions the Directive also provided the possibility to use the information transmitted by carriers for law enforcement purposes. This includes allowing its use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including the protection of public order and national security as long as it complies with the Data Protection Directive 95/46 (Recital 12 of the API Directive). Pursuant to Article 7 of the API Directive, Member States needed to transpose the Directive by 5 September 2006 and the transposing measure should include a reference to the Directive.

4.2 Intended results and impacts of the Directive as foreseen

The API Directive was to pursue the following two objectives as specified in the Article 1 of the Directive:

- Improve border controls; and
- Combat illegal immigration

Improved border control is intended to be achieved through the advanced transmission by carriers of passenger data to the competent national authorities, who are those responsible for carrying out checks on persons at the external borders. API data allows advance checks on passengers with regard to whether they are legally entitled to enter the EU – i.e. for the identification of irregular migrants from third countries. This can be useful for speeding up obligatory checks on arriving passengers by identifying in advance those who needs further checks (e.g. questioning). With regard to combatting of irregular migration, API data is run against databases which enable to identify persons who should be refused entry at the borders. In addition, under certain circumstances API data may be used for ensuring public order and internal security, implying that persons may be stopped at the border if they are suspected to be involved in activities that undermine internal security.

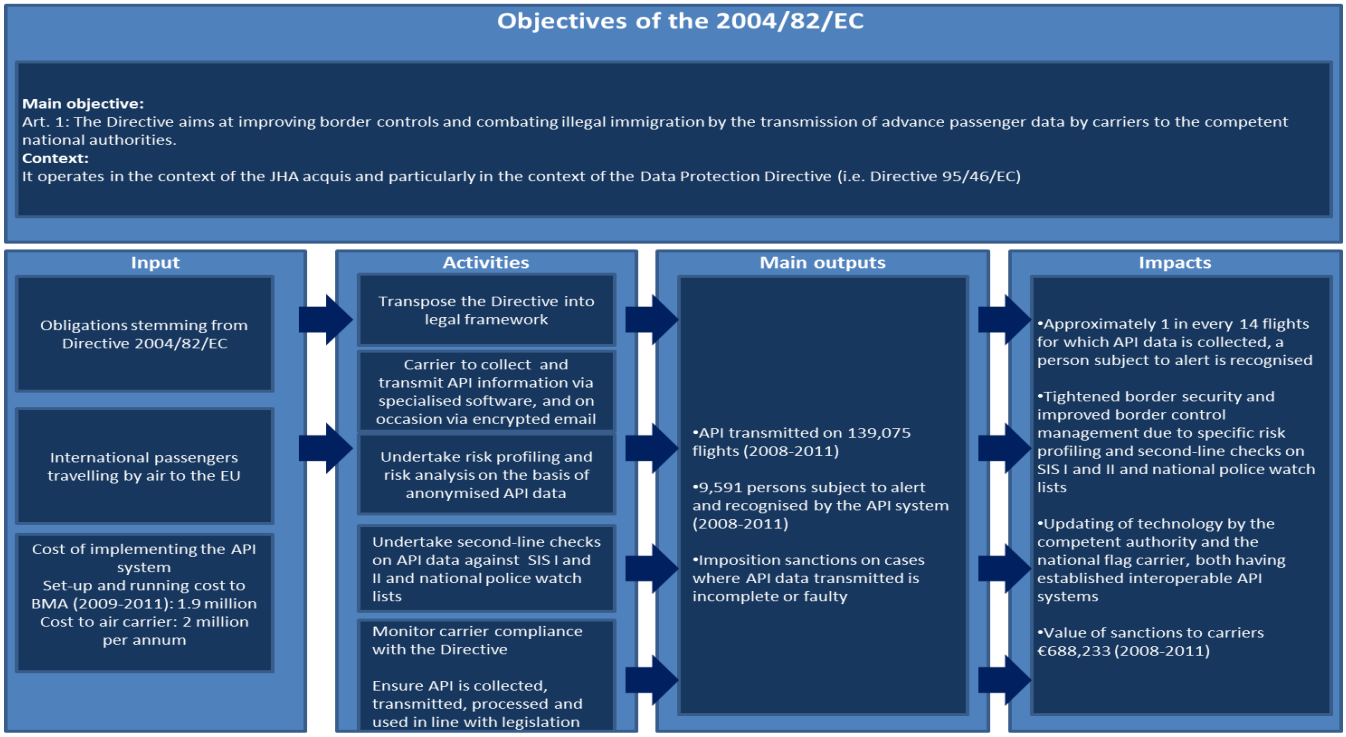
Overall the implementation activities contributing to the functioning of the Directive were expected to yield the following benefits:

- Improved border control (including the possibility to speed up the process and organise it in more effective way)
- Increased effectiveness of combating illegal immigration by stopping the irregular immigrants at the border and helping to identify undocumented people.
- Improved law enforcement capability (when the possibility offered by Article 6.1. to use API for law enforcement purposes has been taken)

4.3 Intervention logic

Figure 4.1 presents the intervention logic diagram for the API system. It has been compiled on the basis information from Germany. It illustrates the input, activities, outputs and impacts achieved by the Directive in Germany.

Figure 4.1 Intervention logic of the API Directive in one Member State



5 Analysis of the quality of the transposition

This section provides a summary of the findings of the conformity study of the transposition of Directive 2004/82 in the Member States. The conclusions presented here are based on the analysis of national transposition studies of the API Directive. The analysis has also been cross-checked with information provided by the Border Management Authorities of each Member State.

The analysis has taken into account the specific situation of some Member States with regards to the Schengen *acquis*. Bulgaria, Cyprus, Denmark, Iceland, Ireland, Liechtenstein, Norway, Romania, Switzerland and the UK all have a particular status when it comes to the adoption and the application of (certain) legal measures building upon the *acquis.* For the purposes of this analysis, the most important issue is the status of the respective Member State vis-à-vis the transposition of the API Directive. Since the situation in each of these Member States raises different issues, a brief explanation for each one is included hereinafter.

- The Schengen *acquis* entered into force in **Bulgaria** and **Romania** on the first of January 2007 (the date when both countries joined the EU). Therefore, the entry into force of the Directive in the territory of Bulgaria and Romania was delayed to January 2007.
- **Cyprus** does not fully apply the Schengen *acquis* due to the particular situation of the island. However, Cyprus is also bounded by the obligation to transpose the Directive, since it enjoys no particular status with regard to it.
- The Protocol on the position of **Denmark** to the Treaty of Amsterdam, the Treaty on European Union and the Treaty establishing the European Community as amended by the Treaty of Lisbon, allows this Member State to decide whether or not it will participate (opt in) in measures building upon the Schengen *acquis.* Recital 13 of the API Directive recalls this and states that Denmark 'shall decide within a period of six months after the Council has adopted this Directive whether it will implement it in its national law'. Accordingly, Denmark notified the Commission of its willingness to participate in the implementation of the API Directive in 2006. However, this participation entails no obligation under EU law, but rather sets up a relationship based on International Public Law rules. Hence, Denmark is not bound to transpose the provisions of the Directive, but rather to implement them.
- According to the Protocol integrating the Schengen *acquis* into the European Union and Council Decisions 2002/192 and 2000/365, **Ireland** and the **UK** take part in the API Directive (Recitals 15 and 16 of the Directive) and, as such, are bound by the obligation to transpose its provisions.
- Pursuant to Council Decision 2008/903, based on Article 15 of the Agreement between **Switzerland** and the EU concerning the association of Switzerland in terms of transposition, applying, and development of the Schengen acquis, Switzerland was required to apply all acts listed in Annexes A and B of that Agreement from 12 December 2008. Directive 2004/82 is part of the acts mentioned in Article 2 (2) of Annex B, and hence, Switzerland is bound to transpose its provisions.
- The Protocol between the **Principality of Liechtenstein**, the European Union, the European Community and Switzerland concerning the accession of the Principality of Liechtenstein to the Agreement between Switzerland, the EU and the European Community concerning the association of Switzerland in terms of transposition, applying, and development of the Schengen *acquis*, came into force by the Law dated 19 December 2011. Article 1 of this Protocol stipulates that the Principality of Liechtenstein joins the Schengen agreement. Pursuant to Article 2 subsection 1 of the Protocol, Liechtenstein is obliged to transpose the regulations named in the Annexes A and B of the Agreement between Switzerland, the EU and the European Community. Annex B of this agreement also includes the Directive 2004/82/EC. Consequently Liechtenstein would have had to transpose the Directive but it does not have an airport. Therefore, it has not been considered in the analysis of the transposition of the Directive.

- **Norway** and **Iceland** are bound by the Schengen Association Treaty signed in 1999 to apply the Schengen *acquis*. According to Recital 14 of Directive 2004/82/EC this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement. Therefore Norway and Iceland are obliged to transpose Directive 2004/82/EC.

5.1 Overview of the quality of transposition

The assessment of the quality of transposition has been concluded on the basis of all the completed transposition studies (31), with the exclusion of Liechtenstein. Hence, the analysis is based on 30 Member States.

The overall quality of the transposition has been assessed on the following basis: whether (i) the transposition was judged to be in full conformity with the Directive and hence in line with *all* its requirements or (ii) whether the non-conformity was judged to be as a result of an incomplete and/or incorrect transposition. The criteria used were:

- Full in conformity: Complete, accurate and correct transposition
- Not in conformity: Gaps in transposition
- Not in conformity: Mostly complete but not accurate/correct transposition

In addition, a separate assessment was made with respect to whether the Member States had adopted any of the two additional measures, namely, the imposition of additional sanctions and the use of API data for law enforcement purposes under certain conditions.

Only one Member State (Slovenia) has been assessed to be in full conformity with the Directive, whereas the remaining Member States included in this analysis have not. Eight Member States[52] have been assessed as not in conformity due to gaps in transposition. Two Member States[53] present an incorrect transposition and the remaining 18 Member States[54] have issues of non-conformity related to both incomplete and incorrect transposition. The above assessment was not applicable to Denmark, since Denmark is not bound to transpose the Directive under EU law.

The main issues of non-conformity relate to data protection and transmission of API data. Twenty-two Member States[55] have been identified as having issues with data protection provisions, mainly related to the length of API data storage and the lack of cross-references to EU and national data protection legislation.

Additionally, the other issues of non-conformity relate to late transposition, gaps in the definitions and lack of cross-references to the Schengen legislation as well as inconsistencies with the minimum and maximum level of sanctions imposed on carriers. More specifically, 17 Member States transposed the Directive later than the deadlines laid down by Article 7 (5 September 2006) and only two Member States transposed all the definitions contained in Article 2. Twenty-one Member States made no reference to the Schengen Convention in their transposing legislation and seven Member States have not transposed the minimum and maximum amounts of sanctions foreseen in Article 4 of the Directive.[56]

Twenty-six Member States have adopted at least one of the two additional measures (ten for the imposition of additional sanctions and eighteen for the use of API data for law enforcement purposes).

All of the above issues are further elaborated below.

[52] BG, CY, FR, ES, IE, NO, RO and SE

[53] EL and LV.

[54] AT, BE, CH, CZ, EE, FI, DE, HU, IS, IT, LT, LU, LV, MT, PL, PT, SK and the UK

[55] AT, BG, CH, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, IT, IS, LT, LV, NO, PL, SE, SK and the UK

[56] A detailed account of the countries will be given in section 5.2.

5.2 Main issues with the transposition

This section reports on transposition issues by theme.

5.2.1 Timeliness of the transposition

With regards to the timeliness of the transposition (5th of September 2006 was the date laid down by Article 7 of the Directive), Member States could be regrouped in three categories:

- Member States that have met the deadline set in the Directive (9);[57]
- Member States that have adopted their transposing national legislation later than the deadline (14)[58];
- Member States for which specific conditions apply or that transposed the Directive in subsequent periods (6)[59]:
  - While Spain initiated the proposal for adopting API rules at the EU level (similar to those that Spain had already in place before the Directive was enacted), it was not until 2009 when some additional information requirements, as well as the legal safeguards concerning data protection, were introduced into Spanish law through Organic Law 2/2009;
  - The UK transposed the legislation partially late with a number of provisions being introduced after the transposition deadline. The main piece of legislation transposing the Directive in the UK is the Immigration, Asylum and Nationality Act, which entered into force in March 2006. However, a number of the provisions of the Directive were transposed in subsequent pieces of legislation (e.g. The Immigration and Police (Passenger, Crew and Service Information) Order 2008 - statutory instrument 2008 No 5- and the Immigration, Asylum and Nationality Act 2006 (Duty to Share Information and Disclosure of Information for Security Purposes) Order 2008 - statutory instrument 2008 No 539-) which came into force afterwards;
  - The transposition of Directive 2004/82/EC was partially late in Hungary, as its Article 4 was transposed through legislation that entered into force in July 2007;
  - Romania implemented the Directive in 2006, but should be considered to have met the transposition deadline, since the country only joined the EU on the 1st of January 2007;
  - The same deadline applied to Bulgaria. However, its national legislation only entered into force in August 2007;
  - Switzerland transposed the Directive in December 2008, in line with the requirements of Council Decision 2008/903, based on the Agreement between Switzerland and the EU concerning the Schengen *acquis*. Hence, Switzerland should also been deemed as complying with the timeliness of the transposition.

5.2.2 Definitions

Article 2 of the Directive provides a number of definitions to clarify the scope of application of its subsequent provisions. The majority of the Member States (i.e. 27)[60] did not transpose one or more of the concepts laid down by Article 2. Only Greece and Ireland included all the definitions in their transposing legislation.

In those instances where the national legislation has not explicitly transposed the definitions of the Directive, it should be reminded that the definitions of the Schengen *acquis* are anyway applicable. Moreover, the absence of definition of 'personal data' could also be considered as non-problematic, since all countries analysed have data protection rules in place either explicitly in their transposing legislation or in an ad-hoc legislative instrument

[57] AT, CZ, FI, FR, IS, LT, SE, SI and SK

[58] BE, CY, DE, EE, EL, IE, IT, LU, LV, MT, NL, NO, PL and PT. Poland implemented the Directive five years after the transposition deadline after an infringement procedure was initiated by the Commission.

[59] BG, CH, ES, HU, RO and the UK.

[60] AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, HU, IT, IS, LT, LU, LV, MT, NL, PL, PT, RO, SE, SK, SL, and the UK

which transposes EU data protection rules.[61] Indeed in cases where no definition of personal data can be found in the transposing legislation, those legal instruments regulating data protection rules in the specific country shall be of application.

Finally, it should be noted that Directive 2004/82 does not explicitly distinguish between third country nationals and EU citizens.[62] However, even though Directive 2004/82 is silent on the matter, Member States are still bound by the EU *acquis* on free movement of persons: EU law on free movement of EU citizens, including Directive 2004/38, forbids systematic checks other than minimum checks on EU citizens who exercise their rights of free movement. Member States are hence not formally obliged by Directive 2004/82 to distinguish between EU citizens and third country nationals but they should ensure that their transposition of this Directive does not breach EU law on free movement of EU citizens.[63] In this regard, it is interesting to note that only three Member States (Belgium, the Netherlands and Lithuania) specifically distinguish third country nationals and EU citizens stating that the transposing national legislation of Directive 2004/82 is only applicable for third country nationals. Two other Member States, Hungary and Luxembourg, have transposed the Directive through legislation concerning 'third country nationals', so the distinction may be inferred. Five Member States[64] do not differentiate between EU citizens and third country nationals when collecting API data. There is no information available for the remaining Member States (20).[65]

5.2.3 Data transmission

Article 3 of the Directive refers to data transmission and contains fundamental provisions of the Directive, by laying down the obligation for carriers to collect and transmit the API data to the relevant authorities (indent 1). Every Member States analysed, except for Iceland, has transposed this requirement in a more or less adequate manner.

Indent 2 of Article 3 contains the list of the API data and establishes the obligation of carriers to transmit it to the competent authorities by the end of the check in. Member States could stipulate an obligation for carriers to collect categories of data that go beyond what it is established in the Directive as the list of API data is not exhaustive.

Only Norway has not transposed the obligation of carriers to transmit data and Iceland requires the data to be transmitted no later than 12 hours before arrival instead of by the end of the check in, which raises doubts about which kind of data are they considered to be, since API data are, by definition, those transmitted immediately after check-in.

As for the lists of API data in national legislations, they vary to some extent as some Member States did not consider the list of Article 3(1) as exhaustive. Seven Member States[66] have chosen to introduce additional requirements that range from the point of exit of the transport means (EE, FI, FR) to the issuing country of the travel document (EL, HU, UK). Finland and Hungary require the carriers to transmit information on the potential statelessness of the passenger. Greece, Hungary, Italy and the UK also collect data on the expiration date of the travel document. Some other categories of data can be demanded, such as the place of transit of the means of transport (Hungary), duration of the flight (Italy) or gender of the passenger (the UK).

As regards indent 3, most States did not explicitly transpose this provision. Here, the Directive requires national legislation to refer to Art. 26 of the Schengen Convention as supplemented by Directive 2001/51 (obligation of carriers to check the documents of third

[61] i .e. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[62] The issue has been raised by a number of Members of the European Parliament in the last few years (E.g., Parliamentary Questions E-2115/07, P-4788/07, E-6080/2008, E-0509/10 and E-3162/10). A clear interpretation of the scope of the API Directive on this regard has still not been officially expressed.

[63] See response from the European Commission to Parliamentary Question E-6080/08.

[64] EE, EL, ES, IT, SI.

[65] AT, BG, CH, CY,CZ, DE, DK, FI, FR, IE, IS, LV, MT, NO, PL, PT, RO, SK, SE and the UK

[66] EE, EL, FI, HU, IT, RO and the UK

country nationals to entry in the EU and obligation to carry them back in case of illegal entry). The lack of cross reference can be considered as a minor compliance issue since the obligations imposed by the Convention and Directive 2001/51 are anyway transposed in national legislation in all bounded Member States can be categorised as follows with respect to this obligation:

Table 5.1 Categorisation of Member States with regards to Art. 26 of the Schengen Convention and Directive 2001/51

Member States referring to Art. 26 and/or Directive 2001/51		Member States with no reference to Art. 26 and Directive 2001/51 but which have included these provisions in the API transposing legislation		Member States with no reference to Art. 26 and Directive 2001/51
Member States with explicit reference	Member States referring to corresponding national legislation	Member States where the text of the Schengen rules is directly included in the same article transposing Art.3	Member States where the text of the Schengen rules is included in different articles	BE, BG, CH, CZ, DK, EE, FI, FR, HU, IE, IT, IS, LT, LU, LV, NO, PL, RO, SE, SK and the UK
DE, ES	EL,MT,PT and SI	NL	AT, CY	

5.2.4 Sanctions

Article 4 lays down the fines to be applied in case of breach of the obligations set in the Directive. Transposition of, alternatively, the minimum or the maximum amount for fines is required. Two issues have been identified with regards to Article 4:

- The second part of indent 1 'Member States shall take the necessary measures to ensure that sanctions are dissuasive, effective and proportionate (…)' has not been explicitly transposed in any Member State. This may derive from the fact that, under national law, sanctions should be anyway, as an intrinsic characteristic, dissuasive, effective and proportionate. Therefore, in practice, no problem might arise.
- With respect to the transposition of the minimum or maximum amount of the sanctions (Article 4.1. a) and b)), the national reports flagged whether one or the other amount has not been transposed. As stated above, the Directive only requires Member States to transpose either the maximum or the minimum and hence, in cases where only one has been transposed, no problems of overall conformity of this provision really exist. Twenty-three Member States[67] have transposed either a maximum or a minimum amount (or both) falling within the thresholds laid down by the Directive. Cyprus, France and Poland have established the exact amount of the fine, and this has been considered as a correct transposition of Art. 4.1. a) or b) since these amounts are within the limits provided by the Directive. Seven Member States[68] have not transposed either a minimum or a maximum amount or have transposed amounts (either lower or higher) that do not correspond with those established in the Directive.

5.2.5 Proceedings

Article 5 of the Directive states that 'Member States shall ensure that their laws, regulations and administrative provisions stipulate that carriers against which proceedings are brought with a view to imposing penalties have effective rights of defence and appeal'. This provision has not been literally transposed in any Member State. However, it has been considered that

[67] AT, BG, CH, CY, DE, EE, EL, ES, FI, FR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SI and SK.

[68] BE, CZ, DK, IS, SE, NO and the UK

the essence of the Article was transposed whenever a reference to the rights of defence and appeal as enshrined in the general national system was made (i.e., the national transposing legislation provides a reference to other legislative instrument where this right can be found). In this respect, the Member States can be categorised as follows:

- Twenty-one Member States[69] have a provision in the transposing legislation that makes a reference to the rights of defence and appeal in their legal systems.
- Nine Member States[70] make no specific reference to the rights of defence and appeal in their transposing legislation. However, this might not constitute a problem in practice, since the rights of defence and appeal are anyway enshrined in the more general legal framework of each of the concerned Member State.

5.2.6 Data processing

Article 6 of the Directive contains the provisions governing the processing of the API data. The majority of the data protection rules applicable to the handling of API data are contained in this article which is therefore of particular importance for the analysis of the quality of transposition. Article 6 intends to align the level of data protection applicable to API data to the standards of the Data Protection Directive 95/46, to which it refers several times.

In order to define a clear analytical framework for the examination of the transposition of Article 6, the two main obligations provided for by this article have been considered: provisions governing the exchange of API data and provisions relating to data protection issues. Within these categories, each obligation included in the Article has been analysed separately.

Provisions governing the exchange of API data

The first paragraph of Article 6.1. states that:

'The personal data referred to in Article 3(1) shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks with the objective of combating illegal immigration more effectively.

a. Transmission to the competent authorities: 26 Member States[71] have reflected, in their national legislation transposing Article 6.1., the obligation for carriers to transmit the data to the competent authorities. Only Bulgaria, Denmark, Greece and the UK do not mention this obligation in the part of their national legislation pertaining to the transposition of Article 6.1. However, in practice, carriers are obliged to transmit the data to comply with all the other provisions of the transposing legislation and therefore the problem of non-compliance seems minor.

All the 26 Member States mentioned above specify that the transmission shall be done to the authorities in charge of border control. With regards to the specific authorities to which data are transmitted, Member States can be categorised as follows:

Table 5.2 Categorisation of Member States on the basis of which authorities are transmitted the API data

Member States using a general definition ('BMA - Border Management Authorities' or 'Authorities responsible for checks'	Member States specifying the authorities		
AT, BE, ES, FI, HU LT, LV, NL, NO, PL, PT, RO and SI	National police forces as	Immigration officer	Ministry of Interior

[69] BG, CY, CH, CZ, EE, EL, ES, FI, FR, IS, IT, HU, LT, LU, MT, NO, PL, SE, SI, SK and UK.

[70] AT, BE, DE, DK, IE, LV, NL, PT and RO

[71] AT, BE, CH, CY, CZ, DE, EE, ES, FI, FR, HU, IE, IT, IS, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SI and SK

Member States using a general definition ('BMA - Border Management Authorities' or 'Authorities responsible for checks'	Member States specifying the authorities		
	immigration authority		
	CZ, DE, EE, IS, IT, LV, SE and SK	CH, CY and MT	IE and FR

b. For the purpose of facilitating border checks: from the 26 Member States transposing the obligation to transmit the data to the competent authorities, 14[72] mention that this transmission shall be done for the purpose of facilitating border checks. Spain does not expressively mention this purpose, but it can be inferred from the wording of the transposing provision. On the other hand, 12 Member States[73] do not state that the data shall be transmitted for this purpose. The UK establishes that the data are likely to be used for immigration purposes but does not specify that they can be used to facilitate border checks.

c. With the objective of combatting illegal migration: among all 30 analysed Member States, 14[74] specify in their transposing legislation that the data shall be transmitted for the purposes of combating illegal immigration. The remaining 16 Member States[75] do not mention this purpose in their transposition of Article 6. However, 13 out of these 16 Member States (all except for Bulgaria, Denmark and Greece) refer to the fact that the data shall be transmitted to border management authorities (see above), which remit includes fighting against irregular migration. Furthermore, the objective of combating irregular migration is normally mentioned in the preambles of the respective transposing instruments.

The second paragraph of Article 6.1 reads:

'Member States shall ensure that these data are collected by the carriers and transmitted electronically or, in case of failure, by any other appropriate means to the authorities responsible for carrying out border checks at the authorised border crossing point through which the passenger will enter the territory of a Member State […]'.[76]

a. Electronic data transmission: almost all Member States analysed (i.e. 25)[77] have correctly transposed the requirement of electronic data transmission. Some minor compliance problems have been identified in Ireland and the UK, where no reference to 'other appropriate means' of transmission has been done. Switzerland allows for alternatively transmitting the data by paper.

Five Member States[78] have no mention in their national transposing legislation of the need to transmit the data electronically. The requirement to transmit information electronically, although not transposed correctly in the countries mentioned above, might not lead to problems if in practice this is what happens. However, if transmission still happens manually, it may hinder the effectiveness of the API systems. A throughout analysis of the way transmission is done in each Member State has been carried out in Section 6 below, dealing with implementation.

[72] BE, CH, CY, CZ, EE, ES, FI, IE, LU, NL, PL, PT, RO and SE

[73] AT, DE, FR, HU, IS, IT, LT, MT, NO, SK, SI and the UK

[74] BE, CH, CY, CZ, DE, EE, ES, FI, HU, IE, NL, PL, RO and the UK

[75] AT, BG, DK, EL, FR, IS, IT, LT, LU, LV, MT, NO, PT, SE, SI and SK

[76] The obligation to save data in a temporary file will be analysed in the next subsection on provisions relating to data protection issues.

[77] BE, BG, CH, CY, CZ, DE, EE, EL, ES, FI, FR, IE, IS, IT, LT, LU, LV, MT, PL, PT, RO, SE, SI, SK, and the UK

[78] AT, DK, HU, NL and NO

Provisions related to data protection issues

Article 6 provides for a number of conditions in order to guarantee an adequate level of data protection in line with the provisions of the Data Protection Directive 95/46/EC. It should be clarified that the conformity checking of the national provisions with the data protection *acquis* is outside the scope of the present study, therefore this analysis did not look at whether or not the Member States have transposed correctly the provisions of Directive 95/46/EC on data protection mentioned in this Article. Instead, national experts have checked whether or not the national transposing legislations make reference to either the Data Protection Directive or their transposing national legislation on data protection in line with obligations set under Directive 2004/82/EC.

For the purposes of this analysis, four main obligations[79] have been identified.

- The obligation for the authorities to save the data in a temporary file (Article 6.1, second paragraph);
- The obligation for the authorities to delete the data within 24 hours after transmission unless the data are needed for exercising their statutory functions in accordance with national law and subject to data protection provisions under Directive 95/46/EC (Article 6.1, third paragraph);
- The obligation of carriers to delete data within 24 hours of the arrival of the means of transport (Article 6.1., paragraph four); and
- The obligation on carriers to inform the passengers in accordance with the provisions laid down by the Data Protection Directive, and in particular, in accordance with Articles 10 (c) and 11(c) (Article 6.2).

These four obligations are intertwined. The relevant connections have been taken into account in the analysis below.

a. Obligation for the authorities to save the data in a temporary file: thirteen Member States[80] make no reference, in their transposing legislation, to the obligation for the authorities to store the data in a temporary file. However, for the majority of them[81] this may not pose any problem in practice since they have transposed the requirement for the authorities and the carriers to delete the data within 24 hours of transmission/arrival of the means of transportation (see below). In these cases, the temporary character of the file can be inferred. Austria, Czech Republic and Iceland, on the other hand, allow for storing the data for longer than 24 hours and this, coupled with the lack of mention to a temporary file, could constitutes an issue of non-conformity.
b. The obligation for the authorities to delete the data within 24 hours after transmission unless needed for statutory functions respecting data protection provisions: ten Member States allow the authorities to store the data for longer than 24 hours[82]. None of them, except for Lithuania,[83] mentions that the data can be kept for longer than 24 hours only for 'statutory purposes'. Austria, the Czech Republic, Denmark, Estonia and Slovakia do not mention a specific time limit for data storage. Furthermore, the Czech Republic, France, Italy, Lithuania and Slovakia allow the authorities to keep the data for longer than 24 hours for purposes that go beyond the statutory functions linked to border checks as established by Art. 6.1. France allows for the storage of data for up to 5 years for undefined purposes other than the fight against irregular migration. The UK also allows the authorities to keep the data up to

[79] The last paragraph of Article 6.1 (the use of API data for law enforcement purposes) will be analysed in Section 5.2.7 on additional measures.

[80] AT, CZ, DE, EE, FI, FR, IS, HU, LV, LT, NL, PL and SE

[81] CZ, DE, EE, FI, FR, HU, LV, NL, PL and SE

[82] AT, CH, CZ, DK, EE, FR, IT, LT, SK and the UK

[83] Lithuania mentions the statutory purposes only as one of the purposes for which data can be kept for longer than 24 hours. Its national transposing legislation allows waiving this time limitation also for 'securing public order and national security' which fall beyond the statutory functions of the border management authorities.

5 years. Italian legislation foresees the possibility to keep the data for six months for undefined law enforcement purposes which could be broader than the one intended by the Directive. Switzerland provides for the possibility of storing the data for longer than 24 hours for 'statistical purposes'. The incorrect transposition of this provision has been deemed as a major non-compliance issue since the time limits are establish in order to ensure that API data are handled in a manner that does not affect the fundamental data protection rights of the passengers concerned.

With regards to the respect of data protection provisions, among the ten Member States allowing for storage for longer than 24 hours, as mentioned above[84], none makes any mention to data protection legislation when transposing Article 6.1. Nineteen Member States[85] all comply with the timeline of 24 hours established in the Directive. However, some minor non-compliance issues have been identified among them: none of these 19 Member States includes a cross-reference to the Data Protection Directive in their transposing national legislation. However, seven Member States[86] do refer to their respective national legislation transposing Directive 95/46 and hence, no problem may arise in practice. However, since data protection rules are transposed in all Member States, no implementation problems shall arise.

c. The obligation of carriers to delete data within 24 hours of the arrival of the means of transport: seven Member States[87] do not comply with the obligation for carriers to delete the data within 24 hours of the arrival of the means of transportation. In Denmark, France, Iceland, Norway and the UK, the provision has not been transposed into national law. Austria allows carriers to keep the data for 48 hours. Poland establishes that carriers can storage API data for more than 24 hours when they (…) 'are necessary to carry out [their] business activities', which does not seem to be in line with the requirements laid down by the Directive.

d. With regards to the obligation on carriers to inform the passengers in accordance with the provisions laid down by the Data Protection Directive, the Member States can be categorised as follows:

Table 5.3 Categorisation of Member States with regards to the obligation of informing passengers of API collection

Member States which have transposed the obligation		Member States which have not transposed the obligation
Cross-reference to data protection legislation	No cross-reference to data protection legislation[88]	AT, DK, FI, IS and NO.
BE, BG, CY, CZ, DE, EL, FR, HU, IT, LT, LU, NL, PT, RO, SE and SI	CH, EE, ES, DE, IE, LV, MT, PL, SK and the UK.	

5.2.7 Possible additional measures foreseen by the Directive

The Directive provides for the possibility to adopt the following additional measures:

- Imposing additional sanctions to carriers for serious infringements of their obligations (e.g. seizure, immobilisation, withdrawal of the operating license etc…) (Article 4. 2)
- Using the API data for law enforcement purposes[89] (Article 6.1. final)

[84] AT, CH, CZ, DK, EE, FR, IT, LT, SK and the UK

[85] BE, BG, CY, DE, EL, ES, FI, HU, IE, LU, LV, MT, NL, NO, PL, PT, RO, SE and SI

[86] HU, CY, EL, MT, PT, RO and SI.

[87] AT, DK, FR, IS, NO, PL and the UK

[88] This has been deemed as a minor issue of compliance, since the Data Protection Directive is transposed in all Member States and, as such, shall also be applicable to carriers

Additionally, Recital 8 offers the possibility for Member States to apply the Directive not only to air carriers but also to transport by sea and road. Some countries have chosen to transpose the obligations of the Directive also to non-air carriers since they had legislation covering other carriers as well already in place before the Directive was adopted (e.g., Spain). In Austria, the extension of the Act also to water vessels was implemented in the law before the neighbour states of Austria acceded to the Schengen area. Ever since the accession of these countries, this provision has no scope of application anymore. Others, like Italy, Malta and Iceland, also had previous legislation in place covering other carriers but in these countries the transposition of the Directive has led to a different result: the existing rules still apply to the other carriers while the national measures transposing the Directive regulate now the obligations of air carriers. This implies that in these countries different rules apply to different carriers for transmitting API data.

Only four Member States[90] have chosen not to adopt any additional measures, whereas the remaining 26 Member States[91] have adopted at least one additional measure. Overall, Cyprus and the UK are the only Member States that have opted for more than one additional measure.

In this respect, the following categories of Member States have been identified:

- Those imposing additional sanctions on carriers (10)[92]
- Those using the API data explicitly for law enforcement purposes (18)[93]

1) Additional sanctions

Ten Member States[94] have foreseen, in their national transposing legislation, sanctions going beyond those laid down by Article 4 of the Directive. Five Member States[95] have chosen to impose heavy sanctions such as imprisonment for failure to transmit the data whereas the remaining five Member States[96] have opted for less strict solutions such as seizure or immobilisation. Cyprus, Greece and Spain offer the possibility for the authorities to suspend or withdraw the operating license and/or to mobilise, seize or confiscate the means of transportation. Belgium and Italy allow only for the suspension or withdrawal of the license.

2) Additional objectives and purposes

A binding definition of 'law enforcement' has not been provided by the Directive. For the purposes of the analysis below, 'law enforcement' has been understood in light of Recital 12 which states that: '(…) 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 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 (…)'. However, the understanding of what 'law enforcement purposes' means varies greatly across Member States and no single definition applies when reporting information on the national use of API for this purpose in the study[97].

---

[89] As explained above, law enforcement purposes are understood light of the mentioned Recital 12 be found in recital 12] of the Directive as 'purposes of allowing their use as evidence in 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,'

[90] CH, , PL, SE and SI

[91] AT, BE, BG, CY, CZ, DE, DK, EE, EL, ES, FR, HU, IE, IS, IT, LT, LU, LV, MT, NL, NO, PT, RO, SK and the UK

[92] BE, CY, DK, EL, ES, IE, IT, NL, NO and the UK

[93] AT, BG, CY, CZ, DE, EE, ES, FI, FR, HU, IS, MT, LT, LU, LV, PT, RO and the UK

[94] BE, CY, DK, EL, ES, IE, IT, NL, NO and the UK

[95] DK, IE, NL, NO and the UK.

[96] BE, CY, EL, ES and IT. For more information about the interpretation of this expression, see Section 5.2.7. below.

[97] For further information, please see section 6.5.1.1.

Eighteen Member States[98] have chosen to use API data also for law enforcement purposes. However, the exact nature of the law enforcement purposes is not always as detailed as in recital 12 of the Directive. Moreover, the overall transposition of this additional measure could cause concerns about the treatment of personal data: Article 6.1 requires that Member States opting to use API data for law enforcement purposes shall do so 'subject to data protection provisions under Directive 95/46/EC'. However, among the eighteen Member States that have made use of this possibility, only three (Iceland, Portugal and Romania) include an explicit reference to their national legislation transposing the Data Protection Directive in the provision allowing for use of API data for law enforcement. The remaining Member States[99] allowing for the use of API data for law enforcement purposes do so without any particular reference to data protection rules. This widespread lack of reference to data protection rules may lead to problems linked to the practical handling of these data on the part of the authorities.

[98] AT, BG, CY, CZ, DE, EE, ES, FI, FR, HU, IS, MT, LU, LV, PT, RO, SK and the UK

[99] AT, BG, CY, CZ, DE, EE, ES, FI, FR, HU, LT, LU, LV, MT and the UK

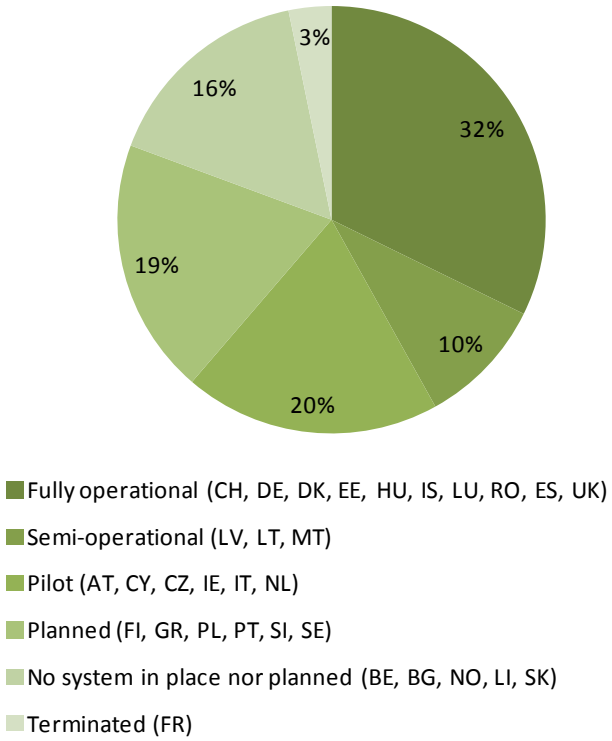
6 Analysis of the quality of the implementation

This section provides an overview of the API systems implemented in the Member States. The findings describe the implementation and functioning of API systems factually without explicit judgments on how these systems conform to wider EU legislation. The information presented is based on the findings of interviews with national stakeholders (border management authorities, data protection authorities and ministries, as well as industry) and the results of the online surveys for the national competent authorities and air carriers.

6.1 Overview of the level and timeliness of implementation

Nineteen Member States[100] currently implement API systems – this represents 62% of all Member States covered by the Directive.[101] In addition, six Member States[102] plan to launch API systems in the short-term. Five countries[103] neither have API systems in place nor have any plans to implement them in the near future[104]. **France** launched a pilot API system in 2007 on the basis of an application decree to adopt different measures to enhance security and border controls, particularly in relation to the fight against terrorism. It was extended for a further two years in early 2009 and for one more year in early 2011, but ended December 2011. France is now redeveloping its Integrated Border Management system so as to incorporate PNR data flows.

Figure 6.1 Proportion of Member States implementing API systems



Denmark, **Estonia** and **Iceland** had advanced passenger information systems in place prior to the introduction of the API Directive. In **Estonia** in 2009 the system was updated to bring it into line with the provisions of the Directive. The system in **Iceland** has been in place since

[100] AT, CH, CY, CZ, DE, DK, EE, HU, IE, IT, IS, LV, LT, LU, MT, NL, RO, ES, UK

[101] This includes Liechtenstein, which is covered by the Directive, but which – as highlighted in Section 5 has no airport and so cannot introduce the provisions of the Directive as they mandatorily apply to air travel.

[102] FI, GR, PL, PT, SI, SE

[103] BE, BG, NO, LI, SK

[104]

2002. **Germany** launched its API system in 2008; it operates on specific air routes only. **Hungary** launched its API system towards the end of 2007 / beginning 2008 and is managed by the Airport police. **Luxembourg and Romania**'s systems were launched in 2008 and 2009 respectively. **Spain** had its system in place already prior to the adoption of the Directive, and the **United Kingdom** were also making plans to implement their initial (pilot) API system 'Semaphore' at the time of the adoption. **Switzerland's** system is not yet fully established. It was launched in 2011, but will be updated from summer 2012.

Latvia implements an API system however, it does not have a centralised API system implemented and maintained by the State. Instead carriers send passenger data to the SBG via e-mail or fax or (in the case of the recently nationalised AirBaltic) via a specific system set up for this purpose. **Lithuania** implements a non-automatic API system, [105] but it is not clear what exactly this entails. In **Malta** no API system has been set up per se; however, the legislation transposing the Directive can be used by the authorities to request advanced passenger information on an ad-hoc basis, when considered necessary for combating irregular migration.

Six countries (AT, CY, CZ, IE, IT, NL) have pilot API system in place. **Austria's** pilot system was launched in 2010 and currently operates out of Vienna Airport only. Federal Police Directorate at Vienna International Airport is primarily responsible for the system. The **Cypriot** system is also a pilot which was launched more recently in 2012. The **Czech** pilot system has been in place since 2006; however an update to the system is planned in 2012 to make it more automated and to enhance its functionalities. **Italy** launched its API system in September 2011 and it is still in the trial phase. API systems were launched in the **Netherlands** in January 2012 and in **Ireland** in early 2012.

Six countries (FI, GR, PL, PT, SI, SE) do not (yet) have API system in place but plan them for the near future. **Greece** plans its API system for later in 2012. **Poland** and **Slovenia** plan to implement API system in 2013. **Portugal** has been implementing a pilot API collection system since 2011, which has involved four air carriers (TAP, Portuguese Airlines, British Airways and SATA). It is awaiting approval of the legislation to regulate the system before the API system is officially launched. **Sweden** plans to implement an API system in 2015. **Belgium** and **Slovenia** do not currently implement API system either, but there are no plans to implement one in the near future.

Table 6.1 Status of API systems in the EU

Member State	Status of API system	Date of launch of system (where relevant)
Austria	Pilot	2010
Cyprus	Pilot	2012
Czech Republic	Pilot (soon to be updated)	2006
Denmark	Fully established	API system for maritime carriers in place prior to adoption of Directive – API system for air carriers is more recent.
Estonia	Fully established	2009 (system in place prior to this, but updated in 2009 to align with API Directive)
Finland	Planned (2013)	N/A
France	Pilot	2006 (ended 2011)[106]
Germany	Fully established	2008
Greece	Planned	2012
Hungary	Fully established	2007 / 2008
Iceland	Fully established	2002

[105] This information is taken from the National Stakeholder Interview with the Lithuanian Border Management Authorities.

[106] France intends to reintroduce API in 2012 to be implemented together with the PNR.

Member State	Status of API system	Date of launch of system (where relevant)
Ireland	Pilot	2012
Italy	Pilot	2011
Latvia	Non-centralised system	2007
Lithuania	Non-automatic system	N/A
Luxembourg	Fully established	2008
Malta	Ad hoc system implemented	N/A
Netherlands	Pilot	2012 (January)
Poland	Planned	Expected 2013
Portugal	Planned	N/A
Romania	Fully established	2009 (August)
Slovenia	Planned	Expected 2013
Spain	Fully established	2003
Sweden	Planned	Expected 2015
Switzerland	In progress	2011 (October)
United Kingdom	Fully established	2004 (Semaphore – pilot API system) 2011 (e-Borders)

Source: interviews with competent authorities

6.2 Overview of the different types of API systems

This section provides further details as to the processes applied in the various API systems that have been implemented in the Member States. The first subsection provides an overview of the main or most common characteristics of API systems. This is followed by description of the positioning of the API systems within integrated border management systems.

6.2.1 Overview of the characteristics of API systems

The way systems are implemented vary in terms of their purpose, their scope, the type of data they collect, the extent to which it is automated and the type authorities having access to it, as well as in terms of the data retention period. The extent of these variations is described throughout the remainder of this section.

Table 6.2 provides an overview of these characteristic.

Table 6.2 Characteristics of API systems

Main elements	Description
API data collected[107]	▪ All Member States (collect the data outlined in the API Directive) ▪ Some Member States (e.g. CZ, DE, HU) collect additional data – e.g. on flight routes, gender, expiration date of travel document.
Passenger information	▪ Carriers are responsible for informing passengers of the processing of their data in all Member States
Capture of API from carriers	▪ Captured through processing of travel documents and/or booking information ▪
Carriers'	▪ The point of transmission (i.e. whether it occurs at check-in, on boarding, or

[107] As recommended by API guideline – ICAO 2011. At minimum the API should include information recorded in Article 3 of the API Directive.

Main elements	Description
transmission of API to Member State authorities	after departure) varies notably Member State to Member State. ▪ Data is sent via specialised software systems (e.g. those provided by companies such as SITA, ARINC, etc.) or via encrypted email or other means (e.g. fax, pdf, non-encrypted email) ▪ Data is sent usually in UN-EDIFACT format, although this is not the case for all Member States ▪ Data is sent via 'push', 'batch' or 'online' method see section 6.4.5 – further analysis into the methods used by implementing states is on-going
Degree of automation	▪ Eleven Member States (CY, EE, FR, DE, HU, IT, LV, LU, RO, ES, UK) implement automatic systems for the transmission of API. ▪ Six Member States (AT, CZ, DE, HU, RO, CH) (also) receive API through non-automated means
Use – processing of API data	▪ In all Member States API data are used by border guards to prepare in advance for border checks of passengers. ▪ In most Member States API is also checked against 'watch lists' or specific databases, such as the Schengen Information System (SIS), Visa Information System (VIS), or national databases (such as police databases). ▪ In Cyprus, API is not checked against any watch lists.
Access to API data from Member State authorities	▪ Data is transmitted directly to border authorities in most Member States or to the police (DE, LU) ▪ Automatic access is granted only to the authority that first receives it in many Member States (except EE, HU, IT, LU, CH, UK) ▪ Other authorities generally have to request access, or obtain access in relation to a particular 'alert' – e.g. if an individual listed
Retention of API	▪ Data is retained only for 24 hours in nine Member States (AT, DE, FR, IT, HU, IE, LU, RO, ES, CH) although they may be kept for longer if they are needed in DE, FR, HU, RO and CH. ▪ If used for law enforcement purposes data may be retained from 1 month up to five years dependent on the Member State's regulatory framework. ▪ In **Germany**, law enforcement authorities may only receive and retain API (retention *period not specified*) on request only if the request is made within 24 hours. ▪ In the **United Kingdom** all API data is retained for five years and may be archived for a further 5 years for the purposes of law enforcement and migration whether the passenger has matched a 'hit' or not.
Criteria and other elements for ensuring that API system comply with Data protection regulations	▪ Data protection authorities oversee the transposition of the API Directive, implementation of API systems and on-going operation of API systems in most Member States ▪ Systems for passenger redress (either via the DPA or through the court system) exist in Member States

Source: interviews with competent authorities

6.2.2 Positioning of API systems within integrated border management system

The API system is integrated into the wider border control system in six Member States[108]. In **France** under its pilot API system, API was used alongside the Schengen Information System and the database of wanted persons for risk analysis as different elements of the French border management system. Now France is currently developing a system that will integrate API with a proposed PNR system. In the remaining implementing countries, API

[108] AT, DK, EE, DE, RO, ES, UK

systems are not integrated into the wider border management system. **Hungary** recognises the lack of integration of its API system as a problem causing inefficiencies in border controls. In **Czech Republic,** the stand-alone system is being developed with SITA and an integrated system will be introduced in the second half of 2012. By contrast, the system in Iceland is dedicated, hence – while it is not integrated into other systems – this is not seen as a negative.

Table 6.3 Level of integration of API into border management systems

Member State	
Austria	Integrated
Cyprus	Non-integrated
Czech Republic	Non-integrated (*currently – although will soon be integrated*)
Denmark	Integrated
Estonia	Integrated
Germany	Integrated
Hungary	Non-integrated
Iceland	Non-integrated
Ireland	Non-integrated
Italy	Non-integrated
Latvia	Non-integrated
Lithuania	*No info*
Luxembourg	Non-integrated
Malta	Non-integrated
Netherlands	Non-integrated
Romania	Integrated
Spain	Integrated
Switzerland	Dedicated / standalone
United Kingdom	Integrated

Source: interviews with competent authorities

6.3 Analysis of the scope of API data collection

This section describes the scope of data collection as part of the API systems, including the range of vessels covered, the targeting of API data collection on specific routes/countries, the proportion of third country national affected by the data collection and the types of data fields collected.

6.3.1 Types of vessels covered by the API system

All implementing countries request API data from air carriers. Legislation in three Member States (AT, ES, UK) also allow for the possibility of collecting API from other vessels (see Section 5.2.7). In practice, three Member States (DK, ES, UK) request API from maritime carriers. Danish border authorities collect API from all ferries arriving from third countries, but only from a few selected flights arriving at Copenhagen airport. Under **Austrian** legislation, API may also be collected from water vessels arriving from the external borders but not to transmit them in advance[109]. **Finland** intends to collect API from air carriers only initially, but is likely also to collect it from passengers entering the Member State via train from Russia. In

[109] The idea to include water vessels in the system took place before new Member States acceded to the Schengen area. Since then these vessels are still mentioned in the law but the rationale have been rendered obsolete by EU enlargement.

the **Netherlands**, discussion is on-going with regard to the collection of API from ships and trains.

In at least five Member States (IS, LV, PT, RO, SE), similar systems for collecting advanced information of passengers arriving in the country via sea exist, but these are subject to legislation distinct from the national measures transposing the Directive. For example, the Icelandic Coast Guard is responsible for coordinating the collection of API of passengers arriving via sea, whereas the border management authority at Keflavik International Airport collects API from flights. In **Latvia**, the national legislation covers only transport by air; however, a similar system - the SafeSeaNet system, legislated by the 'on Ship Reporting Formalities' law – covers sea transportation. A similar system for overland transport is currently being considered and negations have begun with rail operators. It is expected that it will be difficult to develop such a system for land transport, as land carriers are likely to object to the additional administrative burden. **Romania** also operates a system similar to API at sea borders and in ports. As mentioned in Section 5.2.7, national legislation distinct from the measures transposing the Directive also exists in Iceland and Malta in relation to the collection of API from non-air carriers.

Table 6.4 Range of vessels covered by API systems

Member State	Air	Maritime	Train	Coach / car
Austria	S	L	-	-
Cyprus	S	-	-	-
Czech Republic	S	-	-	-
Denmark	S	S	-	-
Estonia	S	-	-	-
France	S	L	L	-
Germany	S	-	-	-
Hungary	S	-	-	-
Iceland`	S	*s*	-	-
Ireland (from mid-2012)	S	-	-	-
Latvia	S	*s*	-	-
Luxembourg	S	-	-	-
Malta	S	-	-	-
Netherlands	S	-	-	-
Romania	S	*s*	-	-
Spain	S	S	-	L
Switzerland	S	-	-	-
United Kingdom	S	S	L	-

Source: *interviews with competent authorities and responses to the online survey (n = 14)*
Key:
L = Stated in the legislation but not implemented in practice;
S = Transposed in legislation and implemented in practice (i.e. in the system).
s = Implemented in practice but national measures distinct to those transposing the Directive apply.

6.3.2 Targeting of API collection

Some Member States have opted for collecting API data from all non-EU flights, whereas others have opted for a targeted approach covering flights only from certain countries. At least six countries (CY, EE, IE, RO, ES, UK) collect API from all non-EU flights arriving in the Member State. Of the remaining thirteen implementing Member States collect API data only

from selected flights – e.g. those identified as routes 'at risk' of irregular migration, which is shown in Table 6.5.

Table 6.5 Scope of API data collection, by selection of flights

Member State	
Austria	Collects API data from selected non-EU flights[110]
Czech Republic	Currently collects API data from collects API data from 190 flights per week from 19 non-Schengen countries in the south and east – the routes are selected on the basis of risk analysis carried out by border police.
Denmark	Copenhagen airport police select specific flights for API data collection
Germany	The Federal Police Headquarters specify which routes on which there will be an obligation to transmit API each year
Hungary	The Airport Division of the Police select specific third countries or passengers to check based on prior risk analysis and other intelligence
Iceland	*No information*
Italy	Collects API data from flights arriving from countries identified as 'at risk'
Latvia	Border guards select specific third countries or passengers to check based on prior risk analysis and other intelligence
Lithuania	*No information*
Luxembourg	*No information*
Malta	Collects API from airlines on an ad-hoc "need to know basis" as required.
Netherlands	Collects API data from flights arriving from countries identified as 'at risk'
Switzerland	The Federal Office for Migration Consult with the border control authorities and air carriers to determine the routes for which carriers are obliged to transmit data on the basis of risk analysis.
France (*pilot system – now terminated*)	API from passengers on flights operating from 30 third countries on particular 'sensitive' routes (e.g. Syria, Pakistan, Afghanistan, Yemen and Iran).
Finland (*API system planned*)	Intend only to request API from flights flying to and from certain third countries that considered high risk, e.g. India, China, Russia, Turkey and Ukraine.

Source: interviews with competent authorities and competent authority responses to the following question in an online survey: What flights do you collect API data. Please select all that apply: all non-EU flights; (b) Selected non-EU flights; (c) Selected intra-EU flights

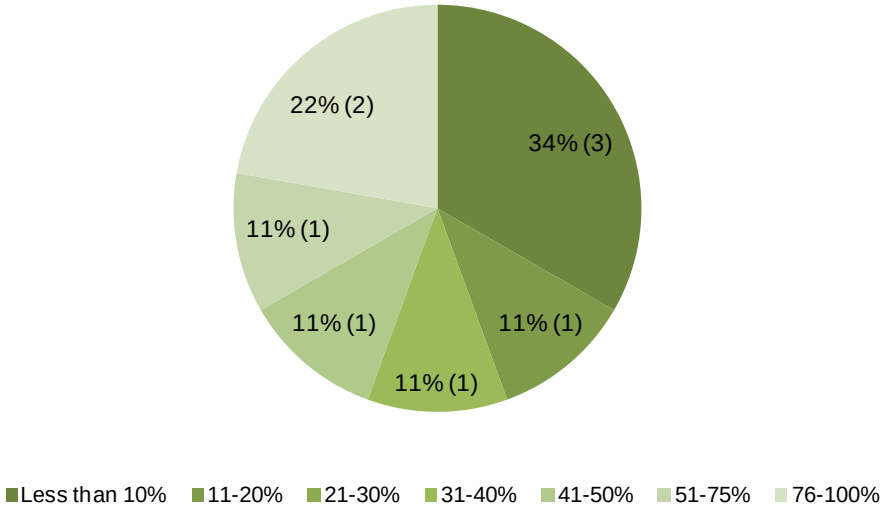
Most Member States only collect information from passengers arriving at the external border (or entering) the Member State, with the exception of **Spain** and the **United Kingdom**, which also collect API of passengers leaving (exiting) the Member State.

6.3.3 Proportion of international passengers affected

Nine respondents to the online survey of national competent authorities (50% of implementing countries) provided information on the proportion of international passengers arriving in the Member States for which API is collected (see Figure 6.2).

[110] See results of the GHK Survey of National Stakeholders.

Figure 6.2 Proportion of international passengers from whom API is collected (*n = 9*)



Source: Competent authority responses to the following question in an online survey what is the proportion of international passengers arriving in your country for which API is collected?

In two Member States (EE, RO) competent authorities estimate that API is collected from 76 to 100% of international passengers entering the county and in **Czech Republic** it is estimated that it is collected for 51 to 75% of international passengers and in **Austria** for 41-50%. In **Netherlands** it is estimated that API is collected from 31-40% of international passengers; in **Hungary** for 11-20% and in **Ireland**, **Malta** and **Switzerland** for less than 10%. This may reflect several issues, such as importance of specific migration routes, API system capabilities, overall national priorities and the geographical position of the country.

Five Member States[111] specifically differentiate in their transposing legislation between third country nationals and EU citizens regarding the collection of API data. Most implementing countries collect API from all passengers, whether they are third country nationals or EU citizens. However, only some of these implementing Member States also process the API data for EU citizens (see Section 5.2.2). The extent to which API data is collected and processed for EU citizens in elaborated under Section 6.5.

6.3.4 Type of data (data fields) collected

All Member States collect the data outlined in the API Directive.[112] In addition, **Czech Republic** collects information on flight routes from carriers, which is used by the Czech border authorities (*Aliens Police*) for proper profiling and risk analysis. **Germany** collects data additional to that required by the Directive (passenger gender and the complete flight route). **Hungary** also collects the expiration date of the travel document used and the code of the country that issued it; the stateless status of the passenger and any place of transit between departure and arrival.[113] The system also highlights when a passenger list has been uploaded after the arrival of the flight or if the number of persons registered at check-in

[111] For more information about the rules on free movement of persons and the collection of data on EU citizens, please See Section 5.2.2.

[112] Article 3 of the Directive stipulates that the following data will be collected: the number and type of travel document used; the nationality of the passenger; the full name(s) of the passenger; the date of birth of the passenger; the border crossing point of entry into the territory of the Member States; the code of transport; the departure and arrival time of the transportation; and the total number of passengers carried on that transport; as well as the initial point of embarkation. Some Member States consider the list of data included in the Directive as non-exhaustive.

[113] **Romania** reports that its 'e-API system also collects information on the number of the flight reservation to show which persons have made the reservation together – however, this is Passenger Name Record (PNR) data and is therefore considered separate to the API system.

does not correspond to the number of passengers. The system also provides statistics – e.g. on the number of flights registered each day, passenger numbers, nationalities, etc. Most Member States collect API in a standard compliant with the UN-EDIFACT format.[114]

6.4 Systems in place for the capture and transmission of API

This section describes the types of API systems in place and mechanisms used for capturing and transmitting API data.

6.4.1 Development of national systems and use of third party systems

Eleven Member States[115] currently implement automatic systems for the transmission of API. Of these, at least three[116] use their own interface for receiving the data, whereas the remainder make use of third parties, such as SITA[117] or ARINC[118] who will receive the API from Carriers and parse it into a compatible format before sending on to the relevant Member States. In **Switzerland** in addition to the SITA system set up, a specific national IT system for data validation and the automatic check of passengers in different databases has been developed. In **Spain** API is received through a nationally developed web service / web application. In **Estonia** API is transmitted/received through server exchange (using both 'push' and 'pull' methods – see below). Systems that use a third party can have quite high transaction costs, particularly if data is transmitted on several frequently operated routes. For example, SITA typically charges the BMA or the carrier by the volume of data transmitted.

6.4.2 Mechanisms and methods for collecting API data

All Member States, implementing the API system, confirm that data is captured by air carriers. The methods of capture vary in the different Member States. API is frequently captured by swiping machine-readable travel documents through 'SWIPE' reader technology; although, as air carriers have not always set up such technology in all third countries, in some Member States[119] accept API which has been typed in manually (see section 6.4.4).

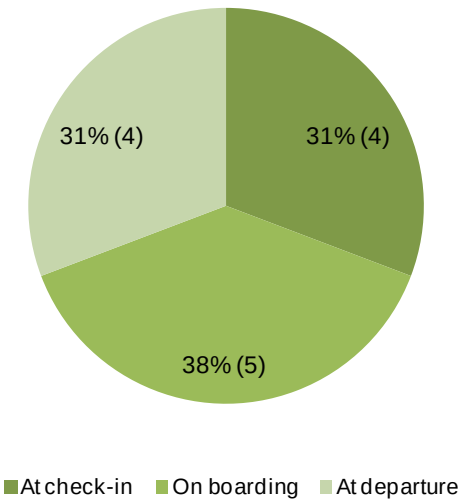
In some Member States the point of capture is at check-in[120], while in others, it is at boarding following ticket inspection[121]. In some countries, data is gathered both at check-in and at boarding, usually depending on the air carrier.[122] In **Germany**, data is captured usually at check-in, however, some of the carriers capture the data only at clearance for boarding. In **Austria**, capture at check-in is preferred because capturing the data after boarding would shorten the time the border control authorities have to check the data which would be inconvenient because many flights are very short (e.g. from the Balkan region to Austria). In terms of transport by sea, in **Denmark** data is collected at boarding but it may also be requested prior to boarding.

6.4.3 Point of data transmission

There is notable variation between Member States as to the point at which data is transmitted to the authorities, as illustrated through the responses from 13 implementing countries responding to the online survey of national competent authorities. Four countries (AT, CZ, CY, HU) transmit API at check-in; a further five (DE, IT, NL, RO, ES) transmit it on boarding; and a further four (CH, EE, IE, MT) transmit it on departure.

[114] This has been reported to be the case in AT, CY, CZ, FR, LU, RO, CH
[115] CY, EE, FR, DE, HU, LU, NL, RO, ES, UK
[116] EE, ES, UK
[117] CH FR, DE, IT, HU, LU, RO
[118] CY, NL
[119] AT, CH, CZ, DE, DK, IS, HU, MT. RO
[120] AT, CH, EE, HU, LU, NL
[121] CY, CZ, FR, LV
[122] SL, RO

Figure 6.3 Point of transmission (*n = 13*)



Source: Competent authority responses to the following question in an online survey: At which point is data transmitted to the authorities in your country?

In **France** API is transmitted either during check-in or after boarding. In the **Netherlands** it is transmitted after the gate has closed. In **United Kingdom,** API can be transmitted up to 30 minutes before departure (i.e. at flight closure – when no-one can get on or off) in some cases; whereas in others, carriers transmit it at the 'wheels up' moment – i.e. on departure. The reasoning behind the assigned point of departure is often dependent on the particular situation of a Member State – for example, data is captured at check-in in **Austria** because many flights are very short (e.g. from the Balkan region to Austria) and hence there is a need to capture the data with sufficient time to transmit this and give border authorities in the destination country time to process it.

In two countries (CZ, ES) API is transmitted at different times dependent on the flight. For example, in **Spain** it is transmitted after departure, but in some cases on boarding and in **Czech Republic** it is transmitted after boarding, but in some cases at check-in.

6.4.4 Level of automation of transmission

Nine Member States[123] currently receive API through non-automated means. Six Member States[124] receive API from carriers via email – in **Malta** this is non-encrypted; however, of these, three[125] plan to work with SITA in the near future. In **Denmark** carriers send API in a structured (compatible) excel format via email to the competent authorities to be entered into specific software system ("Polkon") – which incorporates API, visa, lost documents and biometric data – and the API is then checked against databases automatically. **Hungary** receives API data in various forms including fax, pdf documents, and paper copies – the data is entered manually into the system, but then checked against various databases (see below) automatically. **Cyprus** and **Germany** also receive API via fax. **Ireland** also operates primarily as a manual system for which there will be one border management official responsible.

The border management authority in **Latvia** receives information from its national carrier AirBaltic via a special programme developed for transmitting API in spreadsheet form, which allows for semi-automatic entry into the API system (for facilitated checking against databases), but it receives API from other airlines through fax and email. Due to

[123] AT, CH, CZ, DE, DK, IS, HU, MT. RO

[124] AT CH, CZ, DE, DK, MT - e.g. CZ and CH plan to implement a system of transmission via SITA from 01 July 2012.

[125] AT, CZ, CH

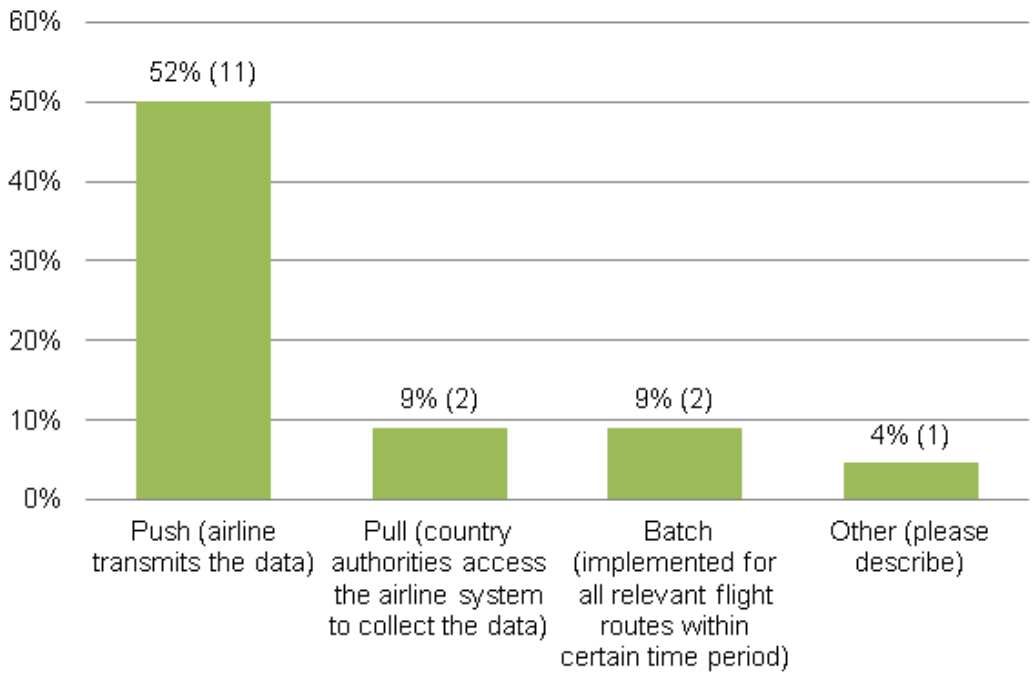
inefficiencies of entering data manually and the time limitations on border guard staff, data from carriers other than Air Baltic is only entered in cases where prior risk assessment or intelligence from the national law enforcement agencies indicate the need for a more detailed check.

In general, automated systems have high start-up costs, but low(er) operational costs whereas manual systems have high(er) staff costs. In relation to data protection, systems which ensure restricted / controlled – e.g. by encrypting API during transmission and limiting the number of staff who have decryption keys – apply higher levels of data protection than those which allow for non-encrypted data to be sent (e.g. via email) or which allow numerous staff to access the data. Some Member States (e.g. Czech Republic) consider an automatic system the best solution for safeguarding personal data, whereas Switzerland states that an automated system is a sensitive issue from a data protection point of view and, when they introduce an automated system in 2012, they plan to amend data protection legislation to allow for the system.

6.4.5 Method of transmission

There are various methods of transmitting API. First API may be transmitted through a 'push' or a 'pull' system. In the case of the former, the carrier sends the data, whereas in the case of the latter the competent authorities have individual access to the carrier's system from which they may 'pull' the API.

Figure 6.4 Method of transmission (*n = 13*)



Source: Competent authority responses to the following question in an online survey: What mechanisms are used for data transmission in your country? (Push, Pull, Batch, non-Batch, other – select all that apply)

According to the online survey of national competent authorities, eleven countries (AT, CH, CZ, CY, DE, EE, ES, HU, IE, NL, RO) implement a 'push method' of transmitting API. The push method was also implemented in **France**. In addition to whether they are push or pull systems, Member State systems may differ as to whether they are 'batch' or non-batch'. The 'batch model' means that API will be requested for selected routes for a specified time period (e.g. all flights on a particular route for a six month period), whereas non-batch means that flights are selected flight-by-flight. The method used in **Germany**, **Hungary, Netherlands** and **Spain** for the transmission of API data is a both 'push' and 'batch' – in the case of the former, air carriers transmit certain API data to the authorities but not to the database of the authorities directly; in the batch method the Police request data only for specific flights which are suspected to be potentially carrying irregular migrants, following a risk assessment.

6.5 Processing and use of API data

This section describes the purposes and focus of processing and use of API data. It also describes the databases against which the API data is checked and the process of carrying out those checks.

As discussed above, the Directive states that the objectives of the processing of API data are the improvement of border controls and the fight against irregular migration. In addition, Member States could opt to use API data for law enforcement purposes in line with Article 6.1*. final*.[126] As previously explained, there is no single definition of 'law enforcement'. From the information gathered during the study, it resulted that 'law enforcement' has taken many meanings from public security, to terrorism to combating serious crime and other less severe criminality. This has blurred the focus of potential data processing purposes. In this respect, Sections 6.5.1 and 6.5.2 describe the uses of API data from the several angles reported by the competent authorities.

6.5.1 Use and processing of API data

6.5.1.1 Purposes for processing API data

Member States who have implemented API systems have done so in order to fulfil a number of different national objectives. All implementing Member States use API for the purpose of border management (i.e. to facilitate the process of border checks) and for preventing irregular migration (i.e. in order to identify any anomalies in the fulfilment of entry conditions or documentation of persons arriving at the border). In **Czech Republic** API partly replaced a system of prior checking of passenger information which the Member State had had to abolish on joining the Schengen Area. In **Estonia** the API system also replaced a system which existed prior to joining Schengen.

As stated in section 5.2.7, eighteen Member States [127] have chosen, in addition to the main objectives of the Directive, to have the possibility to use API data also for what they considered 'law enforcement purposes'. Of these, nine[128] actually make use of API for law enforcement purposes in practice. BMAs in **Ireland** and **Lithuania** have reported that law enforcement purposes were one of the reasons for implementing an API system. In addition, the competent authority in **Spain** has reported that the Member State makes use of its API for law enforcement ("public security") purposes. Table below indicates the types of law enforcement reasons for use of API data and which authorities have access to that data.

Table 6.6 Examples of types of use of API data for law enforcement purposes in Member States

Member State	Extent to which the API system implemented is used for the purpose of law enforcement and which authorities have access to that data
Czech Republic	The use of API data for law enforcement purposes covers prevention of terrorism. In addition, besides the Alien's police, the data can be accessed by the criminal police, other police units or secret services (if requested and justified in writing), for both border control and law enforcement purposes. This is regulated by the internal instruction of the Directorate of Alien Police Service.[129]
Estonia	One of the purposes of implementing an API system is to prevent problematic security situations. In practice, the Police and Border Guard Board process the API data according the State Borders Act §9³ (5) and (6) (which allows for API data to be processed for the purposes of fighting against illegal immigration, border control and law enforcement). The Board is responsible for taking action against passengers with active criminal records and for co-operating with law enforcement authorities in other Member States. The legislation also allows the

[126] For more information about the interpretation of this expression, see Section 5.2.7. below.

[127] AT, BG, CY, CZ, DE, EE, ES, FI, FR, HU, IS, MT, LU, LT, LV, PT, RO, and the UK

[128] AT, CZ, EE, ES, FR, DE, HU, RO, UK

[129] Response to the following question" To what extent the objectives of the Directive are related to the ones of other Directives and/or EU systems/regulations? What are the main complementarities and/or problems arising from these obligations?"

Member State	Extent to which the API system implemented is used for the purpose of law enforcement and which authorities have access to that data
	use of the data by the police, investigative body, surveillance agency and security agency for the purpose of fulfilling their tasks.
France	One of the main purposes of implementing the pilot system in France is to prevent terrorism. The system has enabled authorities to track known people known to the police. Central agencies of the ministry of interior accesses API data for prevention and fight against terrorism purposes.
Germany	In Germany, authorities with competencies of averting danger, serious infringements of individual rights, criminal prosecution or prosecution of administrative offences and execution of convictions can receive and keep API data but only on request and only if the request is within 24 hours from the receipt by the police.
Hungary	In Hungary API data transmitted by air carriers can also be used by the police for procedures that cover criminal or petty offences.
Iceland	The Border Police performs checks on the national database and sends alerts to relevant authorities. The database contains information on persons who are suspected of serious crimes, of going to attempt the kidnapping of a child, who are subject to an arrest warrant or considered a threat to national security or public order. The border police may grant law enforcement officers access to API data, and other authorities including the Directorate of Immigration, as applicable.
Romania	In Romania, API data is used for risk analysis, drawing up risk profiles and taking appropriate measures: the implementation of the Directive offers the possibility for the border authority to undertake risk analysis on the basis of pre-screening of incoming passengers, especially those arriving from countries with high potential risk The Romanian Border Police (RBP) is entitled to take decisions against persons against whom an alert has been issued Data may be kept separately for law enforcement purposes for up to 5 years, inaccessible for first and second line of control in the BCPs and may be made available only on written demand.
Spain	In Spain one of the reasons for implementing an API system was to protect public Security. In Spain API data may be used by the police and the civil guard for intelligence purposes and to fight crime at any level (from terrorism to 'common' crimes)
United Kingdom	The main purpose of implementing the API system in the UK was for law enforcement and the data can be stored for up to five years. API data are used, for example, for criminal investigations and for analysing the patterns and trends in the department of Revenue and Customs. The UK law enforcement authorities made over 11 000 arrests using API data between January 2005 and January 2012.

Source: Interviews with competent authorities (stakeholder responses to the following questions: (a) "To what extent has API data transmitted to national authorities is used, and for which purposes has it been used intelligence, law enforcement, etc. ((b) To what extent has API data transmitted to national authorities is used, and for which purposes has it been used intelligence, law enforcement

As indicated above, API data may be used for identifying persons who are considered as a threat to public order and hence interest to law enforcement authorities. This is for competent authorities to investigate crimes committed by persons who are identified in API lists; to prosecute persons who have committed crimes who are listed on API lists; or to investigate a crime or incident happening under certain circumstances for which information on the passengers on a particular flight may be useful. In **France** API data was collected principally for the purpose of preventing terrorism. Similarly, in **Spain,** one of the main purposes of the API system is to protect citizens against security threats. In **Estonia** the border authorities use it for risk profiling. In **Hungary** the Police can use the data collected to proceed in criminal/petty offence proceedings **Latvia** specifies that the API data may also be used for 'public order' and 'the protection of State security interests'. Law enforcement authorities generally provide intelligence on the individuals that pose a threat to national security before a certain time frame (e.g. time when or event to which such persons could arrive), then SBG checks the API data accordingly and implement closer passenger

inspection, if concrete threats or persons have been identified. In the **United Kingdom** API data is checked against specific watch-lists including those of 'wanted persons' of law enforcement authorities, and if a match is made, an arrest may be made on the passenger's arrival.

Cyprus, Italy, **Romania** and **Spain** also use API data for intelligence (i.e. checks on passengers) and future risk profiling. **Ireland** indicates that, in addition to improving border security, it also aims to improve the 'passenger experience' for bona fide passengers and improve the cost-efficiency of border management in launching its Irish Borders Information System in 2012. The Irish system aims to only allow for the processing of API data for law enforcement purposes in relation to crime occurring at the border (e.g. human trafficking, crimes for which a European Arrest Warrant has been issued). In **Romania** the information is used for elaborating risk analyses of countries which pose a high risk of irregular migration.

6.5.1.2 Scope of processing API data, including data processing of EU citizens

All implementing Member States collect API data from third country nationals and process and use the data to improve border control and combat irregular migration. API data can also be collected from EU citizens, as the Directive did not make a distinction between EU citizens and third country nationals[130]. For practical reasons, when collecting API from a particular flight/journey, most implementing countries collect API from all passengers, whether they are third country nationals or EU citizens[131]. According to online survey and stakeholder interviews at least twelve implementing Member States also process data for EU citizens. Table 6.7 specifies countries that also process API data for EU citizens.

Table 6.7 Member States processing API of EU citizens when carrying out checks

	Also process API of EU citizens when carrying out checks	Do not process API of EU citizens
Austria	Yes	-
Cyprus	Yes	-
Czech Republic	Yes	-
Denmark	*No information*	
Estonia	Yes	-
Germany	Yes	-
Hungary		Yes
Ireland	Yes	-
Iceland	Yes	-
Italy	-	Yes
Malta	-	Yes
Netherlands	Yes	-
Romania	Yes	-
Spain	Yes	-
Switzerland	Yes	-

[130] Five Member States (BE, HU, NL, LT, LU) specify that API is to be collected only on third country nationals. No information is available for other Member States – see section 5.2.2.

[131] Member States are not required differentiate between EU citizens and Third country nationals but they should make sure that their interpretation of the Directive does not preclude EU citizens and their family members to fully enjoy their right to move and reside freely.

	Also process API of EU citizens when carrying out checks	Do not process API of EU citizens
United Kingdom	Yes	-

Source: Interviews with competent authorities and competent authority responses to the following question in the online survey: Do data checks against specified databases cover all passengers, EU citizens included?

Only three countries (HU, IT, MT) reportedly do not collect/process API on EU citizens in practice. It is not clear through what mechanism this is achieved: in the case of **Italy** and **Malta**, this may be because API is processed manually in these countries; however, checks are carried out automatically in **Hungary**, so the system is likely to be more complex. In **Latvia**, API data of Latvian citizens is not checked; this is achieved by means of a specific code or identifier marked against Latvian passengers[132].

Some Member States limit the collection of API s collect information on EU citizen from non-Schengen flights only. **Austria**, **Czech Republic**, **Italy** and **Switzerland** collect information from passengers only on non-Schengen flights. However, this is complicated by the fact that some EU Member States are non-Schengen (i.e. BG, CY, IE, RO, UK) and, for example, **Spain** collects API from flights arriving from the United Kingdom, because the UK is non-Schengen; however, other countries may not wish to collect information on UK flights as UK is an EU Member State. Moreover, the **United Kingdom** collects API of EU citizens and uses these for law enforcement purposes. As the legislation of other Member States stipulates that API cannot be collected for EU citizens, some carriers therefore refuse to collect the data on EU citizens for the UK authorities, to comply with other Member States legislation. **Austria** and **Germany** have pointed out that it could be useful to collect API on intra-Schengen flights. **Austria** also points out that it would be useful to collect API outgoing flights for use for police purposes.

6.5.2 Checks against specific databases and watch lists

In all Member States API data are used by border guards to prepare in advance for border checks of passengers. In most Member States API is also checked against 'watch lists' or specific databases, including national databases and European ones such as the Schengen Information System (SIS) and Visa Information System (VIS). In **Iceland** information on non-nationals living and working in Iceland as held by the Directorate of Immigration, the Directorate of Labour, the police, the tax authorities and the National Registry may be linked together and API checked against it. Furthermore, API is checked against the national 'G-database', which contains information on persons who are suspected of serious crimes, who are banned from entering or leaving Iceland, who suspected of going to attempt the kidnapping of a child, who are subject to an arrest warrant or considered a threat to national security or public order. In **Luxembourg**, an automated system feature for SIS-check is under development.

Table 6.8 indicates the databases and watch lists against which API data is checked. It is clear from the content of some of the databases that the checks can be done for the purposes of border control and fighting illegal immigration as well as on the basis of wider law enforcement activities. SIS I and SIS II for example contain information on warrants (including European Arrest Warrant), entry bans, missing and required persons, criminal offences and surveillance, among others and national police watch lists target wanted persons, including those suspected of criminal activity. However, this does not mean that the data is solely processed for law enforcement purposes as the information can also be used to support decision making regarding preventing irregular migration and/or supporting border control measures. Member States that process API data for EU citizens when carrying out checks (i.e. AT, CH, CY, CZ, EE, ES, DE, IE, IS, IT, NL, RO, UK) are likely to use the data for law enforcement purposes.

[132] Information provided by the Latvian border guard – there is no further information as to how this system functions.

Table 6.8 Watch lists / databases against which API is checked in Member States

Member State	SIS I	SIS II	VIS	National database of non-nationals	National Police watch lists	National justice database	Other
Austria	X	-	-	X	X	X	
Czech Republic	X	X	X	-	-	-	Interpol and up to 18 other databases
Estonia	X	-	X				
France	X	-	-	-	X	-	-
Germany	X	-	Planned	X	X	-	-
Hungary	X	-	X	X	-	-	-
Iceland	-	-	-	-	X	-	The national 'G-Database'
Ireland (from mid-2012)	-	-	-	X	-	-	X (stolen passports)
Italy	X	X	-	-	X	-	-
Latvia	X		X	Only if requested	Only if requested	-	-
Luxembourg	X		-	-	-	-	-
Netherlands	-	-	-	Migration watch lists of Immigration and Naturalisation Authority	-	-	
Romania	X	-	-	-	-	-	National 'alert' database
Spain	X	X	-	*"national databases" (not specified which)*			National entry-exit database
Switzerland	X	-	-		X		Stolen passport database & Interpol
United Kingdom	-	-	-	X	X	-	PNR

Source: interviews and survey with competent authorities

6.5.3 Level of automation of checks

In **Austria**, **Ireland**, **Italy**, **Netherlands**, **Romania** and **United Kingdom** (and formerly in **France**) passenger lists (received electronically and automatically) are checked manually. In **Italy** if there is a match between the passenger list and watch list (a 'hit') then the data may be retained for up to six months; otherwise it is deleted within 24 hours. In the **Netherlands**, this is due to the fact that, as the system is currently a pilot, data is not yet sufficiently reliable to allow for a fully automated system – i.e. checks are carried out manually to ensure there are no/fewer inaccuracies.

Some Member States undertake automated checks on API against other databases. In practice, however, any 'hits' are also manually checked to ensure the correct person was subject to the hit. Table 6.9 below shows the level of automation of checks for 11 Member States that provided information in this respect. The information also shows that checks are mostly carried out against SIS I and SIS II as well as against national police watch lists, whereas checks on EURODAC for example are not undertaken to such a great extent.

Table 6.9 Automation of checks against other databases

Database	Automated	Part-automated	Manual
VIS	CZ, CY, HU	EE, IE	NL
SIS I and II	CY, CZ, ES, RO, HU, DE, NL, MT	EE, IT, CH, IE	AT
EURODAC	CY	IE	RO, NL
National police watch list	CZ, CY, RO, HU, IE, DE, NL, MT	IT, CH	AT

Source: Competent authority responses to the following question in online survey: Please tick the box that best describes the nature of the data checks against the above following databases: (i)VIS, (ii)SIS I and II, (iii)EURODAC, (iv)National police watch list

6.5.4 Alerts and application of API

In most Member States[133] when API matches any entries on a watch list, a warning alert is sent to the frontline border police and this passenger will be targeted for examination on arrival. According to the **Czech Republic**, when the SITA system for transmission replaces the use of email transmission later this year, it is expected that the data will be collected more easily and that air carriers will have lower costs for data transmission.

For example, in **Austria**, API is automatically transferred into a web-based application which is screened manually 'for signs of irregular migration' (e.g. unusual routes) and the names of the passengers are checked against various databases (see above). In **Cyprus** advanced passenger lists are checked for irregular migration only; therefore, it can be assumed that while all passenger are checked, only those of those information on third country nationals is taken into account. The API system in **Romania** allows passengers to be checked on a case by case basis, rather than automatically checking the entire list of passengers. Third country nationals are checked against all databases, while EU citizens are checked randomly. In the **United Kingdom** API of EU citizens is systematically checked.

In **Iceland** if checks lead to a 'hit' against the G-database, alerts are sent to relevant authorities.

6.6 Data protection considerations

Some Member State national authorities[134] commented that they did not foresee any problem with the advanced transmission of passenger information in itself, as the data is the same as that which is required on entry (i.e. at passport control). The main data protection issues, therefore, relate to the length of time for which API is retained and the purpose for which it is used, as well as the number and position of persons who have access to the data. Other data protection considerations – e.g. in relation to automated or non-automated methods of transmission were discussed at the end of section 6.3.2.

1) Data retention periods

As described in Sections 4.1 and 5.2.6, carriers and authorities are obliged to delete API after 24 hours unless needed for statutory functions, respecting data protection provisions. For example, API may be retained for longer if they are needed for the checking of travel

[133] e.g. AT, ES

[134] e.g. FI, UK

documents (DE), searches for persons on the border (DE), for prosecution of offences against the security of the border (DE), prevention of terrorism or law enforcement purposes (FR), if they have been subject to a 'hit' against checked watch lists (IT), or law enforcement purposes (CH).

Similarly, API is retained for only 24 hours for the purposes of migration control in **France**, but for up to 5 years for the prevention of terrorism or law enforcement purposes. By contrast, **Czech Republic,** retain API for up to 3 months for law enforcement purposes and **Luxembourg** law provides that the data can be retained for a period of up to a month. In **Germany**, law enforcement authorities may only receive and retain API on request only if the request is made within 24 hours.

In **Denmark** API collected at the sea borders is retained for 24 hours only, whereas API retained by airport police is retained for a minimum of one year. In the **Netherlands** only API that have led to results (hits) are stored longer than 24 hours and only in an anonymised format that can be used for risk analysis.

In the **United Kingdom** all API data is retained for five years and may be archived for a further 5 years for the purposes of law enforcement and migration whether the passenger has matched a 'hit' or not.

In **Iceland** the length of retention and requirement of deletion are not specified in the national legislation.

Hungary and Romania also report that their national competent authorities may retain API data for longer than 24 hours. This is not clear from their transposing legislation (see section 5.2.6), therefore it may be the case that there is a different legal basis for this retention. In Romania API data may be retained for longer than 24 hours for the purpose of statistical analysis as long as it is anonymised. API data may be also retained for up to 5 years for law enforcement purposes, but in these circumstances it may only be made available if requested in writing. In Hungary, API may be retained for longer than 24 hours for border-control purposes or for criminal/petty offence proceedings.

6.6.1 Data access permissions

Data is transmitted directly to border authorities in most Member States although it is transmitted to the police in **Germany** (to the Federal Police Department) and **Luxembourg** (Grand Ducal Police)[135].

In eleven Member States[136] access to API data is only possible for authorities that initially receive it. Subsequent authorities (e.g. law enforcement authorities such as the police or intelligence services) may access the data in most of these cases, but only on request in four Member States[137]; in the form of 'alerts' sent by the first authority (ES), on a need to know basis by vetted personnel (FR); or if the request is made within 24 hours from the receipt by the police (DE).

In **Hungary**, the airport and ordinary police may access the data. In **Estonia**, the border authority (Police and Border Guard Board) also includes a law enforcement section, which is entitled to use the API data for law enforcement purposes where necessary. In addition, the 'surveillance' and 'security' agencies in Estonia may use the data. In **Luxembourg** other States, international organisations or institutions, in accordance with International law can use API data according to the Luxembourgish law (however it is not clear in practice how) and administrative and judicial authorities also have access to API data. In **Switzerland** the Federal Office for Migration (FOM) implement API systems, but the Cantonal police or border guards carry out checks and otherwise use the API data. The FOM is informed about persons who have matched a 'hit' against checked databases by an automatic alert e-mail.

[135] In some countries (e.g. Hungary) the border authorities are a specific division of the police; whereas in others (e.g. UK) the border authorities and police are completely separation bodies. Here both are considered 'border management authorities'.

[136] AT, CY, CZ, DE, DK, FR, IT, LV, NL, ES, CH

[137] AT, CZ, LV, CH

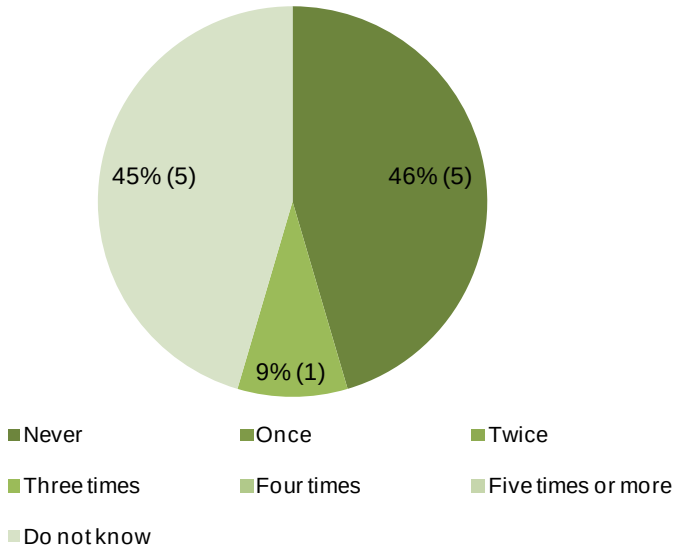
In **Iceland** the police may grant access to API to law enforcement officers, the Directorate of Immigration and other authorities as applicable.

In **Austria** and **Italy** data are checked manually by authorised persons only. In **Austria**, if any API data produces a 'hit' against the checked watch-lists, then information on this passenger will be passed onto the border authorities at the border front line. In **Ireland**, only one initial analyst has access to the API data. This analyst is responsible for passing on information about 'hits' to a liaison officer in the Garda Immigration Office (migration police). The information may then be passed on to 2-3 other officials within the Garda (police) for action to be taken. In **Romania**, data is sent in an encrypted form and is decrypted in a computer disconnected from the Internet. Only accredited personnel have access to the data. In the **United Kingdom** API is sent directly to the national e-Borders Operating Centre (e-BOC) which has a staff of around 120 persons including border authority and law enforcement personnel. These persons have automatic access to the information and produce 'alerts' which are sent on to frontline officers in the border and other authorities. Other law enforcement agencies may also request API.

2) Monitoring and inspection of API systems

Data collected as part of this Study suggests that there is some variation in the way national authorities monitor API system compliance with data protection standards. In at least two countries (DE, RO) API systems are inspected by data protection authorities – in the case of Romania this has happened on an annual basis (three times 2009 – 2012 – see Figure 6.5 below). In other Member States, assessments are either not made (CH, CY CZ, IE, NL) - in some cases likely because the system is only new (CH, IE, NL) – and in others (AT, EE, HU, MT, ES) the national authorities responsible for the implementation of API systems were not aware of whether assessments had taken place or not.

Figure 6.5 DPA monitoring of API systems (according to national authorities responsible for the implementation of API systems) (*n = 11*)



Source: Competent authority responses to the following question in an online survey: how many times the Data Protection Authority in your country has undertaken an assessed inspection of your API system/ database?

6.6.2 Sanctions

Few Member States have imposed sanctions to date. Five Member States[138] report that they have imposed sanctions on carriers. In 2011, the Czech Republic issued sanctions amounting to a total of 934 000 CZK (37 000 EUR). In **Hungary** the average fine imposed as sanction was around 3,000 euro. **Latvia** imposed sanctions in 2008. **Romania** imposed

[138] CZ, DE, HU, LV, and RO

financial sanctions on carriers in 2010 (3 sanctions amounting 2,224 EUR and 1 sanction amounting 4,448 EUR) and 2011 (8,895 EUR – 2 sanctions of 2,224 EUR and 1 sanction of 4,448 EUR[139]); so far no financial sanctions have been imposed in 2012 and in 2009, due to the fact that the system was only in test phase, no financial sanctions were imposed - only a warning was given. In two of these cases, the carrier appealed the decision of the border police in court.

6.7 Analysis of the remit and activities of stakeholders

The remit and activities of the actors involved in the implementation and functioning of the Directive (Ministries, border authorities, data protection authorities, law enforcement authorities, judicial authorities, etc.) is in line with its requirements and with the division of competences set by the national legal systems. The main difference is the extent to which the API systems are implemented by Ministries or border control authorities.

1) Governance arrangements

The most important stakeholders participating in API arrangements are:

- Air carrier(s) ;
- Ministry of Interior / other relevant Ministry[140];
- Border Management Authorities / border police (including 'airport police')[141]
- Other Law Enforcement Authority[142]
- Data Protection Authority[143];
- Judicial authorities (Civil, Administrative, Ordinary, County/District Courts[144]

Other authorities considered important to the implementation of API systems include the Ministry of Foreign Affairs in **Ireland** and **Luxembourg**, the Ministry of Justice, who together with the Ministries of Interior and Foreign Affairs in Luxembourg oversee the API system, and other states, international organisations or institutions, which have access to API system collected in Luxembourg in accordance with International law. In Ireland, the Social Welfare Departments also play a role (see below).

In most Member States it is the border management authorities that develop the API system[145], whereas in others[146] it is the Ministry responsible for border control policy. In some Member States[147] the Ministry of Interior also maintains and administers the API system and the border authorities are only responsible for accessing API data and checking it against watch lists. In **Luxembourg** it is the Ministry of the Interior, the Ministry of Justice and Ministry of Foreign Affairs are competent for enforcing the provisions of the API Directive – i.e. ensuring compliance and imposing sanctions in case of non-compliance.

2) Data reception

API is initially received by border management authorities / border police[148]. In **France** and **Spain**, it is the Ministry of Interior who first receives API and performs the checks against watch lists; they then send any alerts on specific passengers onto the frontline border authorities who will take action (e.g. carry out further checks on the passenger concerned)

[139] The sanctions in RON are as follows: 3 sanctions amounting 10.000 RON and 1 sanction amounting 20.000 RON and 2011 (40 000 RON – 2 sanctions of 10.000 RON and 1 sanction of 20.000 RON. The exchange rate of 1 EUR = 4.49629 RON was used for currency conversion. The exchange rate is based on a rate from 17.09.2012, as published by universal currency converter: http://www.xe.com/ucc/

[140] AT, CZ, CY, DE, HU, IE, FR, LU, ES, UK

[141] AT, CY, CZ, EE, DE, HU, IE. LV, LU, RO, CH, and the UK

[142] HU, LV, and the UK

[143] AT, DE, HU, LV, LU, RO, and CH

[144] AT, DE, HU, LV, and LU

[145] e.g. DE, FI, RO

[146] e.g. AT

[147] AT, FR, ES

[148] AT, CZ, EE, DE, HU, RO

on the arrival of the carrier. In **Switzerland** the Federal Office for Migration (FOM), which comes under the authority of to the Federal Department of Police and Justice, is responsible for the implementation of the Directive, whereas the border police make use of the system and carry out checks. In **Iceland** the border police process API collected from air travel and the state police collect API on sea travel (from the Coast Guards).

3) Data access

Only the authorities who initially receive the API have *automatic* access to the data in many Member States[149]. In the majority of these[150] other law enforcement authorities, or – in the case of France 'vetted personnel' may have access to this on request / on a 'need to know basis' (see section 6.6.1). In the **United Kingdom**, the police (in addition to the border control authority) have a major role in the API system and may access the data.

In **Ireland**, Social Welfare Departments have had a role in the transposition of the API Directive and will have a future role in the API system by providing watch lists. In **Latvia**, the Ministry of Interior has no direct involvement in the API process, but hosts one of the databases (Integrated Inner Information System) with which the API data can be compared. In **Luxembourg,** judicial authorities may access API for judicial / administrative purposes.

4) Passenger information

In all Member States it is the responsibility of the carrier to inform passengers of the use of their data. In most Member States[151] the data protection authority also has a supervisory role in relation to authorising the implementation of API systems and observing the extent to which data protection is met.

5) Sanctions

The authority responsible for dealing with sanctions and appeals also differ from Member State to Member State:

- With regard to data protection, data protection authorities (DPAs) are responsible for receiving and processing complaints from data subjects in nine Member States[152]. In **Germany**, the Federal data protection authority (BfDI) monitors the implementation of the API system, whereas the regional data protection authorities (of the Lander) deal with complaints of data subjects. In **Spain** the Constitutional Court has competence over data protection issues. In **Germany** the API system is inspected and monitored for compliance by the national DPA. In **Italy** the DPA is also responsible for monitoring compliance. In **Iceland** the DPA is in charge of ensuring compliance with data protection rules in general. Some Member States[153] especially reported that passengers may also seek redress in courts – i.e. the civil (AT), local (DE), administrative (CZ), or county (HU) courts. In **Switzerland** passengers may also lodge complaints with the Ministry responsible for border control (Swiss Federal Department of Justice and Police)
- With regard to sanctions against carriers who fail to **comply** with API requirements, in at least seven Member States[154] it is the **implementing** authority that is responsible for imposing such sanctions. In **Estonia**, the courts may also be involved in the sanctioning of carriers. In Spain the Delegate of the Government in Madrid may also impose fines, and fines may also be imposed through **the Administrative** courts.
- Higher administrative courts are attended by carriers in cases of appeals against authorities[155]. In **Hungary**, complaints against the first instance decisions of the police (e.g. in relation to carrier sanctions) are fed up to the National Headquarters of the

[149] AT, CY, CZ, DE, FR, IT, LV, ES

[150] AT, CZ, DE, FR, DE, ES

[151] AT, EE, FR, DE, UK

[152] AT, CZ, IS, EE, FR, DE, HU, LU, ES. In the Czech Republic and Switzerland the data protection authority may also carry out inspections.

[153] AT, EE, DE, HU

[154] AT, CZ, FR, DE, LV, ES, UK

[155] AT, CZ, LU

Police. In Hungary, decisions made by the DPA can be appealed in the ordinary courts. Fines administered to carriers in **Latvia** can be appealed with the Head of the border guards or in the Administrative courts where the carrier is registered. If the carrier is registered outside the country the sanctions may be appealed in the District Administrative Court, the court house in the capital city.

Overall, in most Member States, various authorities share responsibility for ensuring compliance with different elements of API legislation. That is, while ministries or border authorities may be responsible for ensuring the compliance of carriers in transmitting API, data protection authorities are usually responsible for ensuring compliance with data protection provisions, and the courts or judicial authorities are one vehicle for passengers to seek redress.

Table 6.10 Typical remit and activities of authorities implementing and ensuring the functioning of the Directive

Type of authority	Typical remit / activities
Airport and seaport operators	Cooperate with carriers and border authorities
Carrier	Check in passengers Inform passengers of the processing of their data Collect API Store the passenger data temporarily Transmit it to third party (e.g. SITA) / national authorities
Private sector companies	Receive data from airline Parse and re-transmit the data to the relevant national authorities
Border Control Authority	Carry out border checks on passengers arriving / leaving the Member State Respond to warning alerts / 'hits' on the frontline (e.g. by checking passengers who are highlighted as a particular issue, by arresting particular passengers, by contacting the carriers, etc.) *In most cases*: Receive API *In most cases*: Run API against checklists *In most cases*: Release alerts on specific passengers *In some cases:* Impose sanctions on carriers failing to comply *In some cases*: Administer and maintain the system *In some cases:* Carry out risk assessment in order to target particular flights for API collection
Ministry of interior or Ministry in charge of immigration matters	Transposes API into national legislation Oversees the border management authority *In some cases*: develop the API system *In some cases*: administer and maintain the system *In some cases*: receive API, perform checks against watch lists and release alerts on specific passengers *In some cases*: coordinates the other stakeholders involved
Data protection authority	Support the preparation of legislation Approve the system (in terms of data protection) Monitor the system performance to ensure data protection is maintained Process complaints lodged by data subjects Imposes sanctions on processors (e.g. carriers, national authorities) who breach data protection
Regulatory authority (other than DPAs)	Impose fines on carriers
Judicial authority	Courts of appeal for data subjects wishing to complain about data (or other) breaches against carriers Court of appeal for carriers wishing to appeal a decision of the national authorities with regard to API systems *In some cases:* May access API for judicial / administrative purposes
Law enforcement authority	*In most cases:* may make use of API on request and subject to certain conditions. *In some cases:* Send watch lists or advance warnings to the authorities responsible for

Type of authority	Typical remit / activities
	checking API (i.e. the border authorities / Ministry of Interior) regarding persons posing a threat to State security

Source: interviews with competent authorities

6.8 Issues with implementation of API systems and reasons for non-implementation

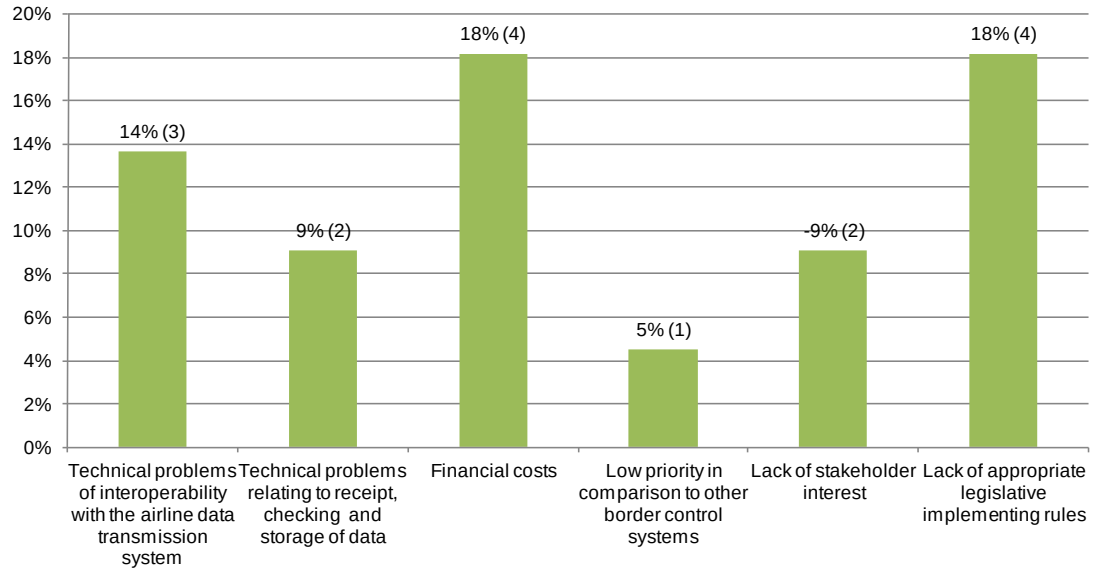
This section outlines the main obstacles to implementation in Member States. In particular it presents the reasons for non-implementation, but also describes some of the issues that implementing countries have faced in setting up their API systems. Recommendations regarding these have been incorporated in section 8 (Conclusions and recommendations) together with all recommendation suggested by the study.

6.8.1 Reasons for non-implementation

The main reasons for non-implementation of API systems relate to technological capacities, financing, political and stakeholder will, and the existence/lack of legislative framework supporting implementation.

Figure 6.6 illustrates some of the reasons for non-implementation as provided by eight non-implementing countries. More information is provided in the subsections below.

Figure 6.6 Reasons for non-implementation (*n = 9*)[156]



Source: Competent authority responses to the following question in an online survey: what are the main reasons for non-implementation?

6.8.1.2 Technical issues

According to the results of an online survey of national competent authorities, interoperability between carrier and BMA systems is a problem in **Belgium**, **Greece** and **Slovenia**. **Belgium** also lists technical problems relating to the receipt, checking and storage of data as an obstacle to implementation, as does **Sweden**. Indeed, in a stakeholder interview, a BMA representative of **Belgium** stated that no API system had been established yet due to the

[156] Responses are from competent authorities in eight non-implementing countries (BE, GR, PL, PT, SE, SI, SK). Two respondents from **Latvia** also gave responses to this question in relation to why the API system in Latvia has not been centralised by the State. The Latvian respondents both stated that lack of stakeholder interest and lack of appropriate legislative implementing rules are reasons for non-implementation, but one of them added that financial costs are also a reason.

absence of electronic system for the collection and transmission of passenger data. Relevant stakeholders had met in 2007 to discuss the API system, but no final decision on how to implement the Directive was reached. Some basic passenger' information is transmitted by some airlines (e.g. for Ryanair flights to Gosselies), upon request by the police. In **Lithuania** and **Norway** passenger data is not currently transmitted electronically, hence the API systems cannot be fully implemented. **Finland** transposed the Directive on time, but implementation of the API system was delayed due to technical difficulties – mainly that the system planned by the authorities was not compatible with the data systems used by the airlines. The carriers system required substantial updating which would have been costly. Finland did not consider it fair to charge the airlines for this, and so the system has taken some time to develop.

6.8.1.3 *Strategic prioritisation and stakeholder interest*

As illustrated in Figure 6.6, low prioritisation (in comparison to other border control systems) and lack of stakeholder interest are also reasons for non-implementation – this is the case in **Slovenia** and **Latvia** (2 respondents) respectively.

Bulgaria, although it has initiated talks with companies who could potentially set up a national API system, is currently prioritising preparations for accession to the Schengen Area and the smooth implementation of the VIS and SIS over the implementation of an API system.

In **Ireland** the API Directive was only transposed in November 2011 and a pilot API system implemented in 2012– both transposition and implementation were delayed by the fact that Ireland is currently processing its draft Immigration Residence and Protection Bill. The original aim was to transpose the API Directive through this comprehensive immigration bill, however due to delays it became unfeasible to do so. The Immigration, Residence and Protection Bill is unlikely to be adopted before 2013.

6.8.1.4 *Other reasons (financial costs, lack of legislative implementing rules, relationship with carriers)*

In four non-implementing countries (BE, GR, LV, SK) the financial costs of setting up an API system have also acted as a barrier to implementation. The competent authority in **Greece** interviewed as part of this Study, argued that the implementation of an API system is costly and that – in the case of **Greece** at least – it does not add value operationally, as the use of API does not eliminate the need for passport controls at airports (which would be a continual cost). In three others (LV, PL, PT) a lack of implementing rules has also caused issues – according to the competent authorities surveyed as part of this Study in Poland and Portugal, this is the only reason for non-implementation. In addition, the competent authority of **Lithuania** consulted as part of this Study reported that there were difficulties in establishing contacts with carriers at the time of transposition which acted as an obstacle to implementation.

6.8.2 Main issues regarding implementation

The main issues that have influenced the quality / ease of the implementation are:

- Issues related to the technical capacity of carriers / third-countries, e.g.:
  - Data capture issues in third countries (e.g. CZ),
  - Inefficient data transmission methods in third countries (e.g. use of fax / email to transmit API by some carriers) and manual entry (e.g. HU, LV),
  - System failures (e.g. CZ),
  - Incomplete data transmission or wrongful transmission (e.g. RO),
- High costs of implementation - particularly for small airlines (e.g. FI, LU, UK),
- Under-development of related systems – e.g. entry/exit systems, SIS and VIS (e.g. CZ, RO).
- Variation in the requirements imposed by Member States on carriers and deviation from international standards (e.g. ES, FR, UK),
- Variation in carriers' methods of transmission (e.g. LV, LU),

6.8.2.1 Technical issues

Romania initially experienced an issue of technical incompatibility between the system of the Romanian Border Police and the system used by air carriers (UN/Edifact format), however, this problem was later resolved. **Cyprus** continues to experience on-going technical issues associated with their recently implemented API system.

In Germany and **Switzerland** while air carriers receive a receipt acknowledging that API has been transferred, carriers are not be informed whether the data is transferred correctly. In **Latvia,** API data are transmitted in three principal ways – fax, e-mail and through a special programme developed by the national carrier AirBaltic. While datasets provided by AirBaltic in the form of spreadsheets can be entered in the SBG system semi-automatically, and compared with all the relevant databases, the data from other carriers must be entered manually and thus is more susceptible to human error and much less time-effective. As a consequence, individuals travelling with fake documents have been only discovered through the semi-automated API process thanks to the AirBaltic data.

6.8.2.2 Other issues

Czech Republic states that, although API is useful, it would be more useful to have the data together with PNR, which is not yet available in the Czech Republic. **Czech Republic** also considers the data retention period of 24 hours too short.

The BMA in **Estonia** consulted as part of this study proposed that it would be useful to harmonise the procedures for transmitting, recording and deleting API data – e.g. by harmonising the format for transmission - throughout the European Union as this would simplify data-transmission procedures for air carriers. However, the BMA further suggested that each State should be left with its own approach on risk assessment, including profiling etc.

7 Results and impacts of the Directive

This section provides the results of the Directive and its implementation according to the evaluation criteria: Relevance, Effectiveness, Efficiency, Impact and Added Value. The information presented is based on the findings of interviews with national stakeholders (border management authorities, data protection authorities and ministries, as well as industry) and the results of the two online surveys for the national competent authorities and air carriers, including a separate data submission on quantitative information on costs and outcomes.

7.1 Relevance

The relevance of the Directive refers to the extent to which its objectives are pertinent to the needs, problems and issues to be addressed and to the extent to which they are coherent with those of API systems in the Member States. The following section covers assessments with respect to:

- The extent to which the intended benefits of the national API systems respond to the needs, problems and issues as identified at national level in the field of irregular migration and border control? Do they match those of the Directive?
- The degree to which the purposes of the API systems created match the objectives of the Directive
- The criteria used to determine the carriers for which API should be applicable?
- The extent to which the obligations related to the implementation of the Directive are in line with other obligations of related Directives (i.e. Data Protection Directive). Are there some issues in terms of coherence and if so what are they (i.e. political, practical issues)?

Relevance of the API Directive is assessed by first addressing the extent to which the Directive responds to the problems and needs identified, and, second, by addressing the extent to which the implementation of the Directive is coherent with other legislative framework in the area.

7.1.1 Relevance of the objectives of the Directive to the needs identified by the Member States

The analysis of the extent to which the Directive addresses the needs of the target groups and stakeholders can illustrate whether there was a clear rationale for the implementation of the Directive, hence, whether the Directive is relevant.

This sub-section considers the relevance of the main objectives of the Directive to Member States. According to Article 1 of Directive 2004/82/EC, the two objectives of the Directive are:

a. Improving border controls; and
b. Combating illegal immigration.

In addition, and as discussed in section 5.2.7, Article 6.1 of the Directive provides for the possibility for Member States to use API also for law enforcement purposes.

The subsection begins by reviewing (i) the perceive needs of Member States at the time of transposing the Directive and the relevance of the Directive's objectives to these needs; followed by (ii) an analysis of the alignment of the national objectives with those of the Directive.

For competent authorities in many transposing Member States (around 52%), at the time of transposition there was a **perceived need to combat irregular migration**. In **Belgium** and **Greece** this was the main need driving the transposition of the Directive. More specifically, in relation to combating irregular migration, Member States mentioned the need of identifying persons with a ban to enter Schengen, identifying persons destroying their travel documents during the flight in order to subsequently claim asylum, identifying document forgeries, etc.

Competent authorities in Member States also identified the **improvement of border management** as a main need. This perceived was mentioned by fewer stakeholders; however, it was identified as a primary need by the competent authorities in **Ireland** and in **Romania** (together with combating irregular migration). For example, Member States mentioned specific national needs, such as ensuring a smooth traffic flow at the air border crossing points, implementing a 'Smart Border' system, enhancing passenger experience, receiving information before the border crossing points in order to enhance the preparedness of border checks, etc.

Last, Member State competent authorities also identified law enforcement as a perceived need at the time of transposing the Directive. For example, the stakeholders consulted reported that combating organised crime, apprehending known criminals, fighting the import / export of illegal drugs and informing intelligence services of potentially dangerous persons and fight against terrorism were amongst the main policy needs at the time of transposing the API Directive[157].

A sample of stakeholders' perceived needs in the area of border control and fight against irregular migration are summarised in the Table 7.1 below and the perceived needs in the area of law enforcement are summarised in Table 7.2.

Table 7.1 Perceived needs with regards to border control and fight against irregular migration (*n =29*)[158]

Type of need	Member States	Total
Combating illegal immigration	AT, BE, BG, CY, FI, FR, GR, HU, IT, MT, NL, NO, PT, RO, SK, UK	16
Border Control Management	AT, CY, EE, FI, IE, IT, LV, MT, NO, RO, SE, UK	12
No pre-defined particular need in this area	CH, CZ, DE, DK, LT, LU, PL, SI	8

Source: National Stakeholder Interviews and Competent authority responses to the following question in an online survey: At the time of transposition (2006) what were the perceived needs, problems and issues to be addressed in your country?

Table 7.2 Perceived needs with regards to law enforcement (*n =29*)[159]

Type of need	Member States	Total
Enhancing Internal security and public order[160]	BE, BG, CY, CZ, EE, ES, FI, NO, PT, SK, UK	11
Fight against terrorism	ES, FR, PT, UK	4
No pre-defined particular need in this area	AT, CH, DE, DK, GR, HU, IE, LT, LU, LV, MT, NL, PL, SE, SI	15

Source: National Stakeholder Interviews and Competent authority responses to the following question in an online survey: At the time of transposition (2006) what were the perceived needs, problems and issues to be addressed in your country?

Hence, **the perceived national needs at the time of transposition largely align with the objectives of the Directive** to (i) combat irregular migration and (ii) facilitate border

[157] This was only mentioned by stakeholders in Member States for which combating terrorism is a long standing tradition.

[158] Responses received from competent authorities in the following Member States: AT, BE, BG, CH, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SK, SI, ES, UK

[159] *Ibid*

[160] The following Member States also identified the need of 'identifying suspects': BE, FI, UK

management. The perceived national needs at the time of transposition also included law enforcement needs, which are exemplified by the adoption of this additional possibility provided in the Directive by eighteen Member States. Almost all Member States recognised the objectives of the Directive as relevant to national needs at the time of transposition, which also matched to the current national needs as identified by national stakeholders.

For some of these Member States (e.g. CZ, HU[161], LT, PL, SI), the Directive was transposed primarily in order to comply with the Immigration and Asylum *acquis* as part of accession to the Schengen Area, and there were no particular national needs, problems or issues that were perceived to be addressed with the Directive. Also, **Czech Republic**, **Denmark** and **Estonia** note that there were already border management systems in place which addressed the needs perceived to be potentially addressed with an API system, hence the API Directive was not perceived to be relevant in this sense. Other Member States (e.g. CH, DE, LU) also reported that there were no specific needs in this area at the time of the transposition of the Directive. A stakeholder for instance mentioned that irregular migration at airports is less of an issue than irregular migration at land border crossings with neighbouring countries, and for this reason the needs could not be addressed through the transposition of the API Directive.

For those Member State competent authorities which did recognise the Directive as relevant to national needs at the time of transposition, the relevance of the Directive to the need to tackle irregular migration in an operational manner[162] but also its relevance to the need to formulate national policy and legislation in the field[163] were both highlighted. The objective of border control was a slightly less relevant objective than combating irregular migration.

Other Member State stakeholders (ES, FR, UK) perceived the Directive as relevant to national needs mainly to the extent that Directive 2004/82/EC allows for the use of API for the purpose of law enforcement. In this sense the Spanish stakeholder commented that the Spanish API system 'goes beyond' the objectives of the Directive in order to meet national needs.

7.1.2 The alignment and relevance of the objectives of the Directive to national objectives

This subsection analyses the extent to which national objectives in transposing the API Directive (and – where relevant – implementing an API system) align with those of the Directive – i.e. the extent to which the objectives of the Directive are relevant in a national context. This analysis supports the overall assessment of the relevance of the Directive.

Generally speaking most Member State competent authorities consulted considered that the objectives of their API systems or legislation were fully in line with those of the Directive. However, some Member States pointed out that in practice because of implementation issues of API systems the intended objectives could not be fully pursued[164]. Implementation issues are fully described in the section on implementation effectiveness (see section 7.2.2). In addition, stakeholders in two Member States (ES, UK) iterated that the national objectives in implementing API systems 'go beyond' those of the Directive, in that use of API for law enforcement purposes is a major purpose for implementing a national API system.

7.1.2.1 The relevance of the objectives to national objectives at the time of transposition

As described in Section 5, the objectives outlined in the transposing legislation in 14 Member States align with the objectives of the Directive – namely (i) to enhance border controls; and/or (ii) to combat irregular migration, although the objectives may not be always worded in exactly the same way as the Directive. More specifically, in 14 Member States data transmission is to be done for the purposes of facilitating border checks and for the purpose to combat irregular immigration. However, in further 13 Member States the legislation

[161] Note that competent authority (the Ministry of Interior) interviewed as part of this Study stated that while *at the time of transposition* Hungary had no particular needs relevant to the Directive, since then, it has become a useful tool for combating irregular migration, hence its inclusion in table 7.1 above.

[162] BE, BG, EE, FR

[163] BG, IE

[164] BE, CY, DK, GR, NO, PT, SI

specifies the data to be transmitted to border control authorities, and as their role in practice encompasses undertaking border checks and combating irregular migration in practice Member States' objectives align with those of the Directive.

In addition, according to their national legislation, 18 Member States have chosen to use API data also for law enforcement purposes.

7.1.2.2 *The relevance of the objectives of the Directive to the purpose of implementing national API systems*

For those Member States which have implemented an API system (or which plan to do so in the near future), the main purposes matched those of the objectives outlined in national legislation, namely:

- To support border management;
- To support the prevention of irregular migration;
- To support law enforcement activities.

Indeed, a number of Stakeholders (AT, CH, CY, DE, HU, GR, LU, MT, PL, RO, SI) consulted as part of this study stated that the objectives of implementing an API system were to comply with the Directive.

With regard to **combating irregular migration**, stakeholders described the following as national objectives (or purposes) for implementing API systems: being informed of irregular migrants being amongst the passengers, disrupting movement of individual who should not be travelling by air, undertaking risk analysis and compiling statistics by travel routes or by profile.[165]

With regard to **border management**, stakeholders stated that the following were amongst the reasons for implementing API: being able to prepare in advance for border checks and evaluating (risk-assessing) passengers prior to arrival; preparing also for any necessary operative measures on arrival of the passengers; increasing the efficiency of border checks by automating the system; improving the passenger experience for bona fide travellers; increasing cost-effectiveness; being able to maximise resource-planning through statistical analysis of API.

With regard to **law enforcement** stakeholders reported that the following objectives were amongst the purposes of setting up API systems: to fight against international crimes, human trafficking, crimes for which an EAW has been issued, etc. The fight against terrorism was seen as relevant by a handful of competent authorities in Member States. For example, in France one of the expected – or intended – benefits of implementing an API system, for example was to obtain information of the itineraries of persons identified as possible security threats. It should be underlined, however, that, the transmission of API data does not prevent the person posing a threat to aviation security from boarding on a plane. This is because API data is collected at departure for the purposes of entry to a Member State and hence transmitted to competent authorities for checking and processing in the Member State of the flight destination. The data processing normally takes place during the flight and any action is undertaken upon arrival. Evidence from the UK however suggests that API data has also been used to stop a suspect person from entering a plane, as they also collect API data on exit. In addition, enabling API system to perform border checks for customs purposes were mentioned by a handful of stakeholders[166].

The perceived objectives of national API systems are provided in the Table below.

Table 7.3 Perceived objectives of API systems (*n = 28*)

Specific objective of the	Member States[167]	International	Air carriers

[165] This information is taken from the findings of the Interviews with National Stakeholders (specifically with the authorities responsible for the API system).

[166] BE, FR, UK

[167] Responses received from competent authorities in the following Member States: AT, CH, CY, CZ, DE, DK, EE, ES, FR, HU, GR, IS, IE, IT, LT, LU, MT, NO, PL, PT, RO, SI, UK

Directive		organisations	
Combating illegal immigration	DK,EE, ES, IT, LT, NO, RO	IATA, IBM	BA, Lufthansa
Border Management	CZ, EE, IS, IE, NO, PT, RO, CZ	IATA	
Law enforcement [168]	CH, EE, ES, FR, IE, LT, UK	IATA, IBM, SITA	BA, Lufthansa
Compliance with the Directive	AT, CH, CY, DE, HU, GR, LU, MT, PL, RO, SI		

Source: National Stakeholder, International Organisation and Air Carrier Interviews, responses to the following question: What were the objectives or purposes of implementing API systems in your Member State? / What are the range of objectives and purposes of API systems has implemented in the Member States?

7.1.3 Criteria for determining the carriers to which API is applicable

As described in Section 6.3.2, in a number of countries (e.g. CH, DE, HU, IT, LV, NL) API is only requested from flights that have been considered 'at risk' of potentially carrying irregular migrants (e.g. if they are arriving from countries identified as source countries for irregular migration). This will also be the case in **Finland** once its API system is implemented.

With regard to the type of vessel, all Member States require API from air carriers, as this is required for by the API Directive (Article 2(a)); in spite of the fact that the Directive does not exclude application of the Directive to other types of vessels. Only **Denmark**, **Spain** and the **United Kingdom** require API from carriers other than air carriers. The reasons given were various. First, a number of authorities implied that, as the API Directive refers primarily to air passenger information, there is little motivation to apply this to other types of vessel. A couple of stakeholders (ES, SE) with only internal borders onto Schengen countries made the point that there would be no reason to require the collection of API at the land borders. Other Member States (e.g. IS, LV, PT, RO, SE) have existing systems in place to collect API from sea passengers; hence there is little value in adapting these to the API Directive system. Finally, a few stakeholders implied that the cost and effort of requiring API from vessels other than air carriers may act as a barrier to the expansion of the system to other carrier types.

7.1.4 Coherence of the implementation of the Directive within the wide legislative context

This sub-section analyses the extent to which the obligations related to the implementation of the Directive are in line with those of related Directives (i.e. Data Protection Directive, Schengen and free movement of persons *acquis*) and report on potential issues.

The Directive is directly related to the following legislation

- Data Protection Directive 95/46/EC
- Schengen *acquis*; and
- Free movement of persons *acquis*

According to the majority of stakeholders consulted as part of this study, the provisions outlined in the Directive do not contradict those found in the above-described legislation. Some Member State national authorities[169] commented that they did not foresee any problem with the advanced transmission of passenger information in itself, as the data is the same as that which is required on entry (i.e. at passport control). However, there was some concern that the application of the Directive in some Member States could lead to issues of

[168] Fight against international crimes, enhancing Internal security and public order, fight against terrorism, prevention of terrorism and get information on the itineraries of some people constituting a security threat to the State, enhancing State security.

[169] e.g. FI, UK

coherence with Data Protection legislation. The main data protection issues, therefore, relate to:

- The length of time for which API is retained and the purpose for which it is used, and;
- The number and position of persons who have access to the data.

Other data protection considerations – e.g. in relation to automated or non-automated methods of transmission were discussed at the end of section 6.3.2.

In addition, as discussed in section 5.2.6, some national legislation does not fully and accurately transpose data protection obligations (e.g. storage of API data in temporary files, obligations (on carriers and authorities) to delete API after 24 hours and obligations to inform passengers). In addition, as discussed in section 6.6, API data is retained for longer than 24 hours in various Member States. Further analysis of the compliance of API systems to data protection obligations is provided in section 7.2.3.4.

Moreover, in relation to data protection, it was suggested that the large-scale processing of groups of data subjects (i.e. passengers) in order to assess potential illegal activity (i.e. irregular migration, persons identified as a risk to national security) risks 'criminalising' these persons, who have not committed anything wrong. A restriction of the scope of application of the API Directive to certain routes or third countries was seen as a potential solution to this risk.

With regard to the impact of the API Directive on the right to free movement of EU citizens; there may be some concerns when API data is systematically collected on intra-EU flights – e.g. in the UK and Spain. As discussed in section 5.2.2, the Directive does not specify that API is only to be collected for third country nationals. Moreover, very few Member States specify this in their national legislation. Hence, as described in section 6.5.1.2, many implementing countries process API of EU citizens. As the EU acquis on the free movement of EU citizens forbids systematic checks other than minimum checks on EU citizens exercising their right to free movement (see section 5.2.2), there is a risk that national legislation and API systems are not fully coherent with the wider legislative context in this respect. The Directive could be amended to provide more guidance on this topic. Moreover, those Member States (e.g. HU, IT, MT) that have API systems in place that only process API of third country nationals (see section 6.5.1.2), could share information with other Member States as to how these systems have been implemented.

In some Member States[170] it is difficult to distinguish between migration and law enforcement purposes in practice when data is used by the same police force. Another stakeholder also pointed out that border checks must still be applied – even when API has been checked in advance – means that the API Directive does not add much value to existing legislation.

In the future, some stakeholders[171] feared that potential coherence issues could arise following the introduction of the proposed PNR Directive. The latter contains an obligation for air carriers to transmit data similar to API data collected through the process of collecting relevant PNR data. The relationship between the PNR and API data could be problematic when the respective objectives of the two Directives are considered. The fight of terrorism and organised crime is the prime objective of the proposed PNR Directive whereas improving border control and combating illegal immigration is the prime objective of the API Directive. Many Member States have taken the position that PNR/API data should be used for both the purpose of fighting illegal immigration and for the purpose of fighting terrorism and organised crime. The distinction made between the two objectives is very complicated to make in practice. Stakeholders also highlighted the need to ensure that the two systems are streamlined and integrated to avoid any technical incoherencies that would cause obstacles to using the two systems together.

[170] e.g. CZ

[171] E.g. FR, HU

7.2 Effectiveness

Effectiveness refers to the extent to which the Directive has achieved its stated objectives. The sections that follow cover the following assessments:

- The extent to which the API Directive has contributed to **improving border controls** in Member States and in the EU
- The extent to which the API Directive has contributed to **combating irregular migration** in Member States and in the EU
- is the degree to which the API data transmitted to national authorities has been used, and for which purposes
- The extent to which the API data collected and transmitted by carriers is compliant with the data requirements listed in the Directive:
  - Are appropriate measures in place to inform the traveller of the collection of their data with respect to: How the traveller is informed on the use of their data?
  - Is information provided to the traveller (e.g. purpose for which data collected, type of data collected, retention period, right of access to data)?
  - Is information on right of access to their data and correction and deletion of such data provided
- is the extent to which the management of API data (i.e. retention and protection) by national authorities and carriers is compliant with the obligations and safeguards for data protection as listed in the API Directive

Effectiveness is assessed according to two different dimensions.

1. The extent to which the Directive has been effective in achieving its 'high-level' objectives; and
2. The extent to which the Directive has been implemented in Member States in an effective manner.

7.2.1 Effectiveness of the Directive in achieving its objectives

The analysis of the extent to which the objectives of the Directive is effective illustrates whether the intended results were achieved in the Member States and allows identifying factors limiting the effectiveness of the Directive. This sub-section considers the effectiveness of the main objectives of the Directive: improving border controls and combating illegal immigration.[172]

The table below summarises the perceived effectiveness of the Directive by stakeholders:

Table 7.4 Perceived effectiveness of the Directive in improving border controls and combating illegal immigration (*n = 17*)

Specific objective of the Directive	Very effective	Somewhat effective	Not effective	Not possible to assess
Combating illegal immigration	DK, ES	BG, CY, CZ, EE, FI, FR, DE, LV, CH, UK	None	AT, IE, LU, NL
Improving Border Control	DK, ES, RO	AT, BG, CY, CH, CZ, FI, FR, DE, LU, LV, NL, UK	HU	IE

Source: Competent authority responses to the following question in an online survey: To what extent the API Directive has contributed to improving border controls in in the EU and its Member States? / To what extent has the API Directive contributed to combating irregular migration in the EU and its Member States?

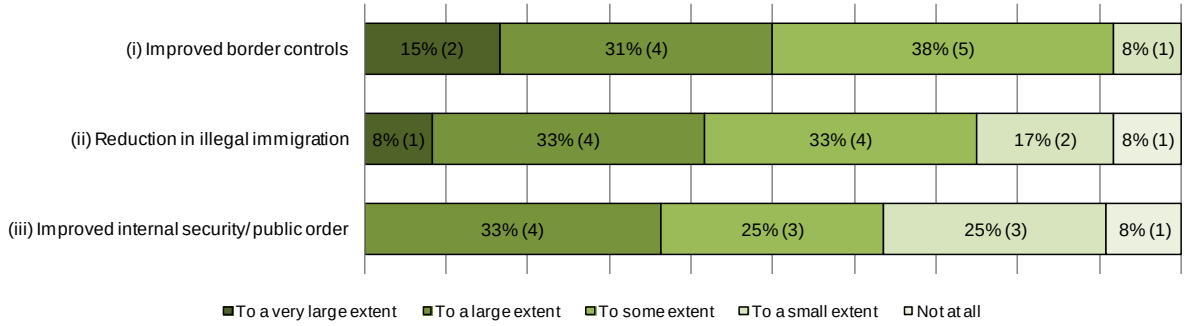
Overall national stakeholders report that API systems have proven useful in achieving the objectives they were set up to address. All national competent authorities consulted had perceived their API system to have facilitated the improvement of border controls and most

[172] This objective is mentioned in Art. 1 of the Directive 2004/82/EC

also expressed the opinion that API systems had contributed to the reduction of irregular migration to some extent. According to national stakeholders, API systems have been less effective in improving internal security.

Indeed, as illustrated in Figure 7.1, most Member State competent authorities consulted as part of the *online survey of national competent authorities* perceive national API systems implemented to have been effective in achieving most national objectives to some extent or even to a large extent.

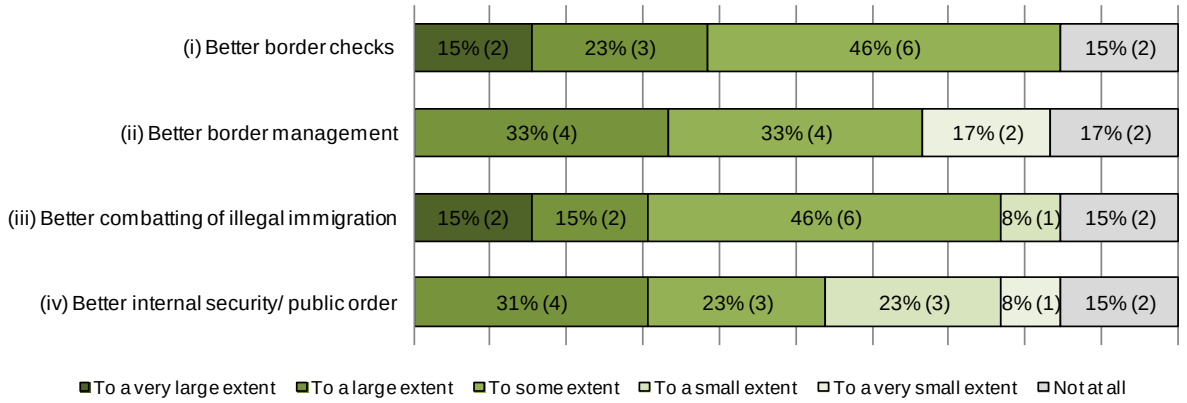
Figure 7.1 National stakeholder perceptions of the extent to which their API system have contributed to the achievement of specific goals (*n = 13*)[173]



Source: Competent authority responses to the following question in an online survey: Please indicate the extent to which, to date, the use of API data has contributed to (i) Improved border controls, (ii) Reduction in illegal immigration (iii) Improved internal security/public order

In addition, the same stakeholders commented on the extent to which API facilitates the achievement of specific goals, such as checks at borders, border management, combating irregular migration and internal security. Similarly to Figure 7.1, stakeholders consulted considered that API systems are most effective in facilitating border checks and combating irregular migration. To a slightly lesser extent, API systems were considered to facilitate border management in general and internal security / public order.

Figure 7.2 National stakeholder perceptions of the extent to which their API system facilitates the achievement of specific objectives (*n = 13*)[174]



Source: Competent authority responses to the following question in an online survey: Please indicate to what extent the API system created in your country facilitates the achievement of the following objectives: (i) Better border

[173] Response received from 13 of the 18 implementing countries: ES, AT, CZ, EE, CY, RO, IT, HU, CH, IE, DE, NL, MT

[174] Response received from 13 of the 18 implementing countries: ES, AT, CZ, EE, CY, RO, IT, HU, CH, IE, DE, NL, MT

checks (ii) Better border control management (iii) Better combating of illegal immigration (iv) Better internal security/public order.

The remainder of this sub-section describes in more detail the extent to which API systems have been effective in contributing to the achievement of the specific objectives of the Directive.

1) Effectiveness of the Directive in combating illegal immigration

Most Member State stakeholders considered that API Directive has somewhat been effective in combating illegal immigration. Reasons limiting the effectiveness are due to:

- The gradual implementation of API systems over the period. Most API systems were tried and experimented over the period and on a reduced scope (i.e. on a sample of third countries, on a sample of Border Crossing Points, or only on some vessels)[175]. The lack of evaluation or factual information on how effective API systems have been in combating illegal immigration. Member States do not hold data on how effective the implementation have been or found it difficult to attribute the effectiveness solely to API data.
- One stakeholder also made the point that, as third country nationals are checked at the border anyway, the added value of API systems in preventing irregular migration is limited.[176]

There is evidence to suggest that API systems have contributed to reducing irregular migration in the following ways:

- By improving risk-based profiling of international passengers[177]. For instance, authorities can now detect illegal practices through risk profiling in a way it was not possible before[178].
- Increasing the rate of detection of persons trying to enter the territory with lost or forged documents[179] especially when they are designated as 'forgers' in the SIS[180];
- For 'blocking' access of irregular migrants attempting to transit external borders via airport hubs– by identifying the main countries of origin of such persons and controlling passenger lists[181] or through the identification of groups of migrants on the basis of the information relating to flight reservations made for several persons[182]; and
- By facilitating the identification of smugglers and irregular migrants. In the Netherlands, in spite of the fact that the API system is only in its pilot phase, several victims of trafficking and smuggling have already been recognised on the basis of passenger data. In the UK, 17,000 passengers have been returned directly in relation to the monitoring of API data, 27 facilitators (i.e. smugglers) have been arrested and 240 lost/stolen passports / travelling documents have been seized over the period 2005-2011.

Competent authorities in Member States also commented on the relative effectiveness of API systems in contributing to various measures to prevent irregular migration, such as risk analysis, return, etc. (see Figure 7.3 below). The findings suggest that API systems are most useful at supporting the targeting of irregular migrants, refusing the entry of suspected

[175] DK, FR, RO, UK

[176] See response of the CH competent authority.

[177] DE, EE, RO

[178] These practices consist in buying a flight ticket to another destination country with a transfer of flight in one EU Member State (e.g. Germany). At the time of transit, some irregular migrant throw away their travel documents and disembark in this Member States (e.g. Germany). Before the Directive came into force it was hard or often impossible to find out the names of these persons and where they came from. Having observed this phenomenon for years the police figured out on which routes this practice is the most prevalent and can "profile" the passengers who are most likely to do this.

[179] DE, LV

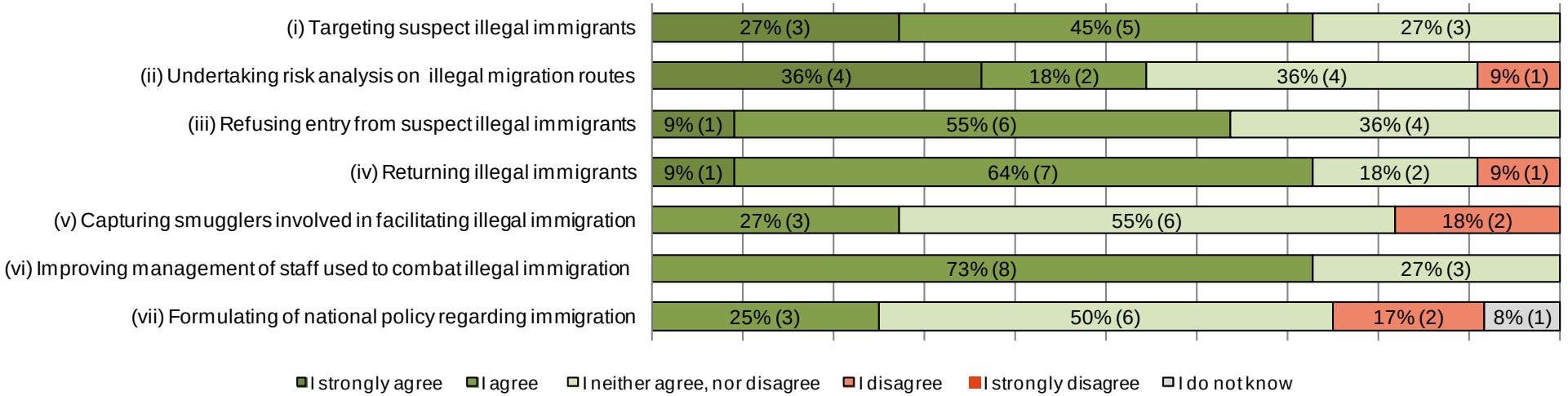
[180] LV only

[181] FR

[182] RO

irregular migrants and improving the management of staff. API systems were perceived to be less useful for capturing smugglers and formulating national policy.

Figure 7.3 Competent authority perceptions of the effectiveness of API systems in contributing to measures to reduce irregular migration



Source: Competent authority responses to the following question in an online survey: Please comment on the following statements: the implementation of API system has contributed to combating illegal immigration in my country with respect to: (i) Targeting suspect illegal immigrants (ii)Risk analysis on illegal migration routes (iii)Refusing entry from suspect illegal immigrants (iv)Return of illegal immigrants (v)Capturing smugglers involved in facilitating illegal immigration (vi)Management of staff used to combat illegal immigration (vii) Formulating of national policy regarding immigration

A number of ways in which API systems could be made more effective in combating irregular migration were also identified by stakeholders. For example, it was suggested by few stakeholders that API systems could be more effective if the data were provided prior to departure so that potential irregular migrants could be identified prior to boarding and thus prevent the irregular migration before it occurred. It was also suggested by competent authorities in Austria and United Kingdom that it would also be more useful to ensure that passengers were aware that the police already possess information on passenger before arriving at the destination.

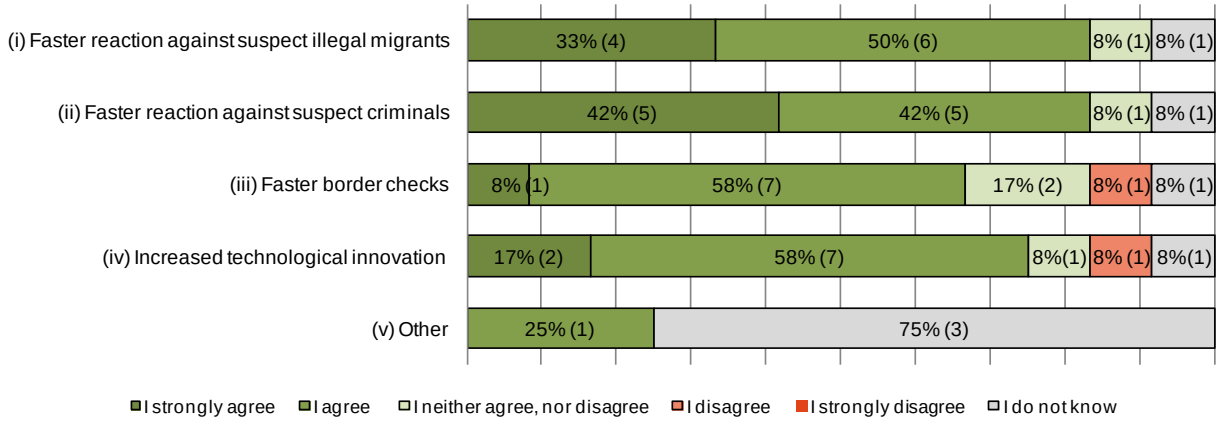
2) Effectiveness of the Directive in improving border controls

As described above, most Member State stakeholders considered that API Directive has somewhat been effective in improving border controls. National stakeholders considered that API systems support resource planning and make the use of border control staff more efficient. For instance, through API systems, competent authorities have been able to:

- Identify specific flights for which enhanced border checks are necessary (i.e. as compared to other flights) because the higher prevalence of non-EU nationals in those flights is known before landing[183];
- Better prepare for the control of specific passengers by identifying them via API data in advance of their arrival. It helps to accelerate border checks because suspected illegal immigrants can be separated from the other passengers and reallocated to separate lanes without the other 'rightful' passengers queuing and waiting[184];
- Anticipate certain situations and anticipate and classify the type of controls to be performed[185];
- Check API data against other databases, and thus shorten the time for controls and checks at the external borders[186].

Indeed, competent authorities in implementing Member States report that API systems have allowed improved the speed with which they can react to the arrival of suspected irregular migrants and suspected criminals (i.e. an efficiency improvement) and have improved border checks in general. Not all national stakeholders agree with this last point, however. Indeed, one industry representative argued that API could be used to reduce waiting times for third country nationals on entering the EU.

Figure 7.4 Competent authority perceptions of the effectiveness of border controls



Source: Competent authority responses to the following question in an online survey: Please comment on the following statements: the implementation of API system has improved border controls in my country with respect to

[183] AT
[184] DE, LU, RO
[185] FR
[186] AT, CH

(i) Faster reaction against suspect illegal migrants (ii) Faster reaction against suspect criminals (iii) Faster border checks (iv) Increased technological innovation (v) Other (option to add their own database and rate it as the others above)

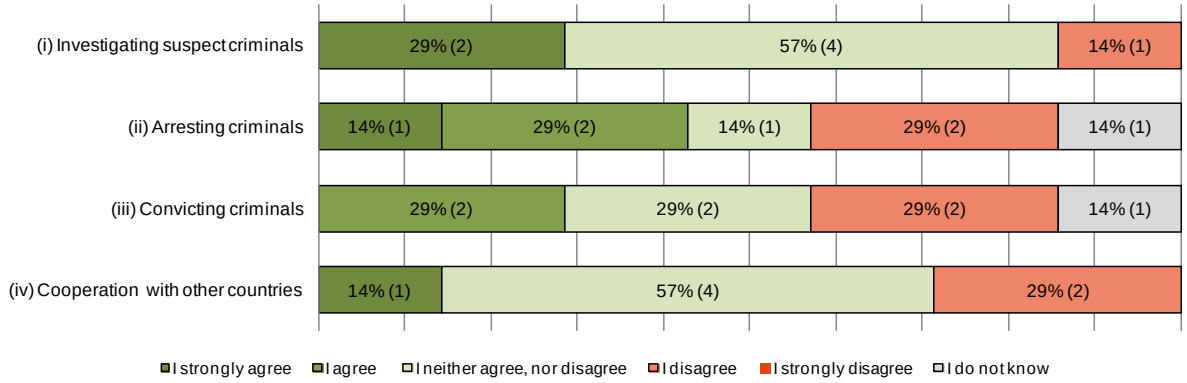
Nonetheless**,** the effectiveness of API systems in improving border controls has been limited to some extent due to the following:

- API systems allow only a limited time (the duration of the flight and a maximum retention time of 24 hours) for the Border Control Authorities to run thorough searches and checks[187]. There is a lack of evaluation or factual information on how effective API systems have been in improving border controls. Member States do not hold data on how effective the implementation have been or found it difficult to attribute the effectiveness solely to API data[188].
- There is a lack of quality of the data in the data transmitted due to manual entries[189];
- API data is a means to an end but not a solution to solving all border control problems. For instance, the border police still have to perform manual checks on passengers and on their personnel data at the external border to verify if they match the API Data transmitted[190].

3) *Effectiveness of the Directive in supporting law enforcement*

As mentioned in Section 5, Article 6.1 provides that - in accordance with their national law and subject to data protection provisions under Directive 95/46/EC, Member States may also use API for law enforcement purposes. In addition to the two main objectives of the Directive, some Member States reported that they have made use of API for enhancing law enforcement. Specifically, they mentioned that this data is potentially useful in preventing crime and terrorism (e.g. FR) and identifying persons who have been identified as a security risk by law enforcement authorities (BE, FI, UK). Competent authorities in implementing countries strongly agreed or agreed that use of API has helped to investigate criminals (AT, RO), arrest criminals (AT, IT, RO) and convict criminals (AT, IT, RO), whereas others (CZ, HU) disagreed. One stakeholder (RO) strongly agreed that cooperation with other countries in the area of law enforcement had improved through use of API, whereas two (CH, CZ) disagreed.

Figure 7.5 Competent authority perceptions of the effectiveness of API systems in enhancing border security and public order



Source: Competent authority responses to the following question in an online survey: Please comment on the following statements : the implementation of API system has contributed to law enforcement in my country with

[187] CH, HU

[188] For instance, one French stakeholder mentioned that the volume of data processed is too small to allow for an overall assessment.

[189] AT

[190] CZ

respect to: (i) Investigating suspect criminals; (ii) Arresting criminals; (iii) Convicting criminals; (iv) Cooperation with other countries; (v) Other (please specify)

7.2.2 Implementation effectiveness

This section reports on the effectiveness of the implementation and functioning of the obligation on carriers to communicate passenger data in Member States. In particular, it provides an assessment of the following:

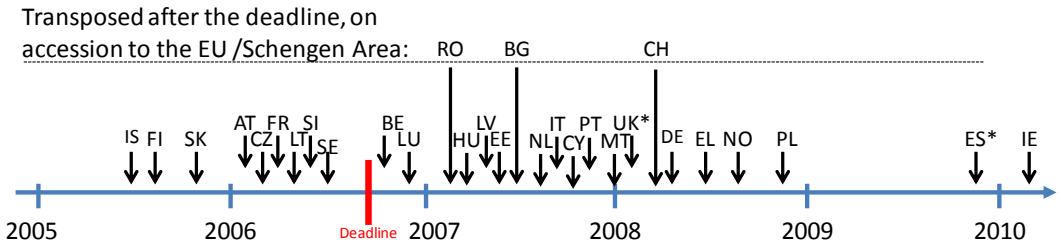
- The timeliness of national transposition of the API Directive
- Implementation of API systems and obstacles to implementation
- The effectiveness of the set-up of API systems
- Compliance of national systems with the requirements of the Directive and other relevant legislation
  - Carrier compliance with data collection and transmission
  - The effectiveness of the application of API
  - The effectiveness of information provision to passengers regarding the collection and use of API
  - Compliance with data protection obligations

7.2.2.1 The timeliness of national transposition of the API Directive

Most of the Member States transposed the API Directive into national law after the deadline for transposition of the Directive (i.e. September 2006). Only nine Member States (AT, CZ, FI, FR, IS, LT, SE, SI, SK) implemented the Directive before the deadline. Spain already had legislation in place prior to the adoption of the Directive which partially transposed it, but did not fully transpose the Directive until 2009. The United Kingdom partially transposed the Directive within the deadline, but completed transposition later. In addition, Romania and Bulgaria joined the EU joined the Schengen Area after 2006 and Switzerland implemented its accession instrument only in 2008; hence while they did not meet the transposition deadline this was for logical reasons.

Figure 7.6 illustrates the timeliness of transposition of the API Directive (date of the last legislative act in force in specific Member States) in relation to the deadline for transposition.

Figure 7.6 Timeliness of transposition of the API directive



*Source: EUR-LEX * indicates the date of full implementation*

There are various reasons for delays to transposition. These may include political considerations, such as low prioritisation and practical considerations, such as the desire to introduce API as part of a 'package' of provisions (e.g. transposing other EU legislation) or the drive to introduce legislation once a pilot has been launched.

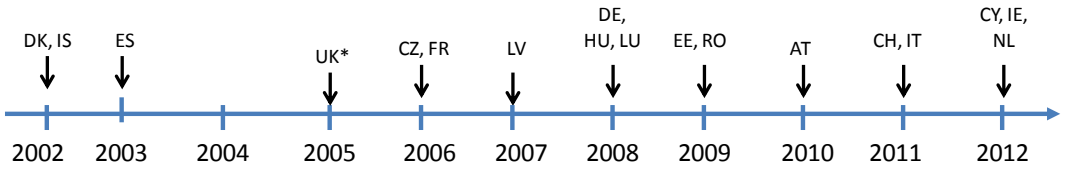
7.2.2.2 Implementation of API systems and obstacles to implementation

The effectiveness of the set-up of API systems has been assessed on the basis of: (i) the extent to which API systems have been implemented by transposing countries; (ii) the extent to which API systems were set up soon after the deadline for transposition of the Directive (i.e. the timeliness of API systems); (iii) the extent to which API systems were set up in the most effective (i.e. cost-effective and efficient) manner.

First, regarding the extent to which API systems have been implemented, as described in section 6.1, over half of the Member States that have transposed the API Directive (20 out of 30) have implemented API systems.[191] Among these ten have implemented it (or will fully implement it in 2012) on a permanent basis;[192] the remaining nine[193] Member States having implemented them on a pilot or semi-operational basis. A further six Member States (FI, GR, PL, PT, SI, SE) plan to implement API systems in the near future.

Second, regarding timeliness, most of the Member States implemented API systems after the deadline for transposition of the directive (i.e. September 2006). Member States that have fully implemented API systems have reported that, it took more than one and a half years to implement a fully operational API system after national legislation had passed. Figure 7.7 indicates when API system became fully operational in the respective EU Member States[194].

Figure 7.7 Timeliness of implementation of API systems



*Source: Member State interviews - * indicates first operational pilot project.*

The main obstacles to API systems implementation were described in Section 6.8. These included:

- Technology:
  - Technology of carriers' reservation, checking and boarding system widely differ;
  - Technology requirements imposed by Member States on carriers are not always in line with internationally agreed international standards. This leads to non-harmonised, redundant and incompatible requirements from authorities worldwide;
  - The above two obstacles make API systems difficult to operate in view of the lack of alignment between carriers' systems and government requirements.
- Financial costs
  - Financial costs and sanctions can be a major hurdle sometimes and especially for small to medium size air carriers with basic or obsolete checking and boarding system;
- Political will
- National legislation

In addition, differences in the interpretation of the API Directive can be a source of problems between the country of departure and the country of arrival. Similarly, there may also be conflicts in terms of data protection legislation in the country of departure and arrival due to differences in legislation or interpretation.

7.2.2.3 The effectiveness of the set-up of API systems

In addition to the obstacles describe above, an industry stakeholder has argued that the fact that the API Directive was drafted without consultations with the industry has meant that it has been difficult for air carriers to implement API systems.

[191] AT, CH, CY, CZ, DE, DK, EE, FR, HU, IE, IT, IS, LV, LT, LU, MT, NL, RO, ES, UK

[192] CH, DE, DK, EE, HU, IS, LU, RO, ES, UK

[193] AT, CY, CZ, IE, IT, LV, LT, MT, NL

[194] Note that the figure only reports on Member States for which date of full implementation of the API system has been obtained through interviews.

Indeed, from an industry perspective the Directive missed the opportunity to introduce API systems that would have brought additional benefits and efficiency savings to air carriers. Such a system would be an 'interactive' API system.

Two broad categories of API systems can be distinguished:

- Legacy API systems[195] which the current Directive allows the implementation of; and
- Interactive API systems which allows governments to check the data of the passengers before they board and hence, to detect any potential security threat or irregular migrant before the flight has taken off.

The second type of API system is considered by industry stakeholders to be more cost-effective and bringing additional benefits in terms of aviation security and cost burdens[196].

As they exist currently, API systems are mainly an advanced warning system implemented to fulfil three types of functions:

- Identifying travellers or passenger planes who are coming at the external borders;
- Allowing for the identification of travellers at the border;
- Performing border management activities (i.e. anticipating border control resources and activities, assessing risk, etc.).

In this sense, it would be beneficial to consider how API systems could be developed to provide benefits also to industry to incentivise the setting up of API systems and their smooth functioning.

Another criticism of the setup of API systems resides in the fact that the Directive encouraged Member States to implement API systems but did not provide guidance on how to do so. This led to a situation where each Member State has implemented an API system whose characteristics and standards differ from those of others. This lack of relationship between Member State API programmes led to a sub-optimal solution where each Member State implemented an API system according to their own standard and requirements. This lack of alignment or harmonisation has had a detrimental effect on carriers' compliance costs and operations.

Additional evidence of the sub-optimality in the set-up of API systems in the Member States were given as follows:

- "The current Directive allows Member States to add further requirements to the API systems, which burdens the industry in addition to introducing legal uncertainties".
- "API systems tend not to be harmonised or integrated";
- "API systems have not been uniformly developed across the Member States. This led to discrepancies in the language and data requirements imposed by Member States to carriers".

7.2.3 Compliance of national systems with the requirements of the Directive and other relevant legislation

7.2.3.1 Carrier compliance with data collection and transmission

Overall the data collected and transmitted by carriers is mostly compliant with the data requirements listed in the Directive. Reasons for failing to comply are:

- Air carrier system failures;
- Incomplete data batches (i.e. missing data) ;

[195] They are based on the provision of passengers data at checking or boarding, transmitted when the plane has departed and on which checks are performed against existing law enforcement or immigration control related databases.

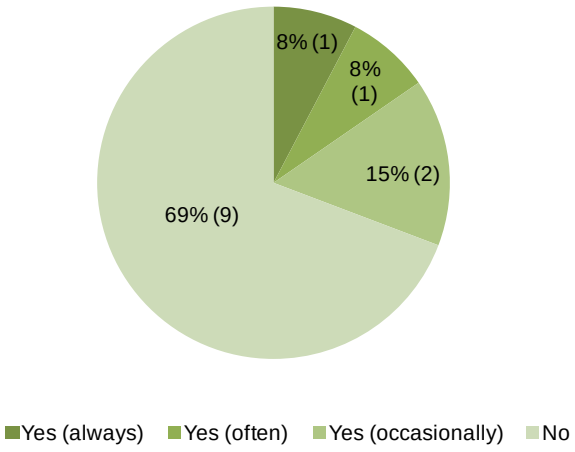
[196] Under such systems, air carriers do not have to bear the cost of return of illegal immigrants because this person would be banned from boarding the plane in the first place.

- Invalid data submission (i.e. wrong date of birth);
- Timeliness of the data transmission (i.e. late transmission);
- Means of data transmission (i.e. paper-based data transmission through fax or e-mails);
- Other difficulties in collecting and transmitting API data, such as in certain countries, airport and telecommunication infrastructures do not allow carriers to collect and transmit the API data in the desired format;

Six Member State competent authorities (AT, CH, CY, CZ, DE, ES) report that have they received faulty or incorrect API data, or find that API data has not been transmitted upon request on occasions (in fewer than half the cases). Two Member State competent authorities (IE, MT) report that they have never received faulty or incorrect data – although this is likely to be because (in the case of Ireland) the API system is only in its pilot phase and (in the case of Malta) because the API system only functions on an ad hoc "needs-based" basis (see Section 6).[197]

Moreover, competent authorities report that they rarely receive data additional to the API data request. Four Member States receive data additional to the original API data request always (NL), often (IT) or on occasion (CH, DE). All four competent authorities stated, however, that they delete it either immediately (CH, DE, NL) or at least within 24 hours (IT). Figure 7.8 presents these responses.

Figure 7.8 Competent authority perceptions of the extent to which additional (non-required) data is sent with requested API (n = 13)



Source: Competent authority responses to the following question in an online survey: Does the data you receive from carriers ever contain additional information to the original API data request?

In addition, national stakeholders interviewed as part of the study reported overall that API data collected and transmitted by carriers is compliant with the data requirements listed in the Directive.

Table 7.5 Perceived compliance of carriers in collecting and transmitting API data in line with the data requirements listed in the Directive (*n = 11*)[198]

	Fully compliant	Somewhat compliant	Not compliant	Not possible to assess
Member States'	AT, DE, EE,	CZ, FR, HU, LV		BG, IE, FI,

[197] These competent authorities were responding to the following question in the GHK Survey of National Stakeholders: *How often do you receive faulty or incorrect API data, or the API data has not been transmitted upon request?*

[198] Responses received from AT, BG, CZ, DE, EE, FI, FR, HU, IE, LV, LU

stakeholder perception on carriers' compliance	LU

Source: Competent authority responses to the following question in the National Stakeholder Interviews: To what extent the API data collected and transmitted by carriers compliant with the data requirements listed in the Directive?

With regard to sanctions, the overall majority of Member States have not imposed sanctions. **Error! Reference source not found.** outlines the Member States which have and – where available – information on the total cost of sanctions.

Table 7.6 Overview of imposed sanctions

Member State	Airline sanctioned	Total cost of sanctions (euro)	Reason for sanction
Austria	*NI*	54,000 euro (2009) 210,00 euro (2010) 45,000 euro (2011)	*NI*
Czech Republic	*NI*	37,000 euro (2011)	*NI*
Germany	*NI*		*NI*
Hungary	*NI*	Average fine of 3,000 euro per carrier	*NI*
Latvia	Turkish airlines	*No information*	Failure to send API Incomplete data sent
Romania	*NI*	50,000 euro (2010) 40,000 euro (2011)	*NI*
Spain	*NI*	*NI*	*NI*

Source: National Stakeholder Interviews and National competent authority data submissions

7.2.3.2 *The effectiveness of the application of API*

Out of thirteen competent authorities in implementing countries that responded to the ICF GHK survey of national stakeholders, only four (AT, CH, CZ, NL) reported that data transmitted by carriers is sometimes not used: three (AT, CH, NL) reported that it is not used on a daily basis and one (CZ) reported that it is not used around once a month. Six other respondents (from CY, EE, HU, IE, RO, ES) reported that API is always processed and used.

Member States generally experienced a lack of effectiveness in using API data at the start of implementing their API systems. This manifested itself in:

- Unusually high number of wrongful alerts due to the screening of API data against the database for wanted persons using wrongfully spelled names or homonyms;
- Authorities dependent on carriers' performance in submitting complete data batches, on time and in the right format.

The perceived usefulness of the data collected was described in section 7.1 in relation to the extent to which API systems had achieved the objective outlined in the Directive. Examples of the type of use of API data are listed below:

- Identifying potential illegal immigrants
- Using API data for border control and other border control related purposes (i.e. make more effective use of border control staff's time);
- Performing risk analyses on main routes used by passengers (profiling purposes);
- Tracking individuals known to the police (i.e. security and intelligence related purposes);

- Enforcing serious criminal offences[199] as well as minor offences related procedures.

7.2.3.3 The effectiveness of information provision to passengers regarding the collection and use of API

In all implementing countries, carriers are responsible for informing passengers of the collection and use of API data. In addition, Member States may use other communications to inform passengers; for example, in the UK, a large ad-campaign preceded the launch of the API system and many Member States provide information on the websites of relevant authorities (e.g. BMA websites). In addition, API systems are now much more common globally - there are over fifty countries running some sort of API systems all around the world – which, some stakeholders have argued, also increases passenger awareness of the collection of API.

However, anecdotal evidence suggests that some passengers are not informed of the use of their personal data[200] and some expressed doubts about data protection of their personnel data. In Hungary, employees working for air carriers and who are in direct contact with passengers are not always aware of the ways air passenger data are collected and used, consequently they cannot provide passengers with accurate information. [201] In addition, as discussed in section 5.2.6, five Member States[202] have not transposed the obligation for carriers to inform the passengers laid down by Article 6.2.

There is also some variation in the time and the manner that passengers are informed. As argued in section 7.1, in some cases, passengers may only be informed of the collection of their personal data once they have boarded the plane.[203] European companies are obliged to inform passengers at the time of purchasing their ticket and passengers need to accept the data protection regulations incorporated in the general terms and conditions prior the purchase of the ticket. For non EU companies, this is done in some Member States on arrival via posters at border control points[204].

7.2.3.4 Compliance of API systems with data protection rules

No major compliance problems with data protection rules have occurred. Overall, stakeholders have not experienced any major problems in relation to data protection, including fundamental rights breaches. Stakeholders also reported that the risk of occurrence is pretty low since Data Protection rules are observed and specific mechanisms have been put in place.

Evidence is as follows:

- There was no issue of this type reported over the evaluation period[205];
- The Directive's provisions and corresponding data protection mechanisms[206] fully respect data protection rules[207];
- There is no risk with the protection of personal data with respect to API systems. The types of data collection and checks enabled by API system would be undertaken even in the absence of such systems, the only difference being that data is received

[199] i.e. including terrorism.

[200] CZ

[201] HU

[202] AT, DK, FI, IS and NO.

[203] See the response of the Hungarian Data Protection Authority (DPA)

[204] FR

[205] ES, FR, LT, LU, MT, SE

[206] Data transmission is transmitted electronically, is encrypted and only accredited personnel have access to API data. Data is kept for 24 hours and after this period. Data are made inaccessible in terms of personal data in an automatic manner. For statistical purposes, only anonymous data are being kept by the system after the expiry of the respective term (RO). Access to API data for law enforcement purposes is available only after making an official written request.

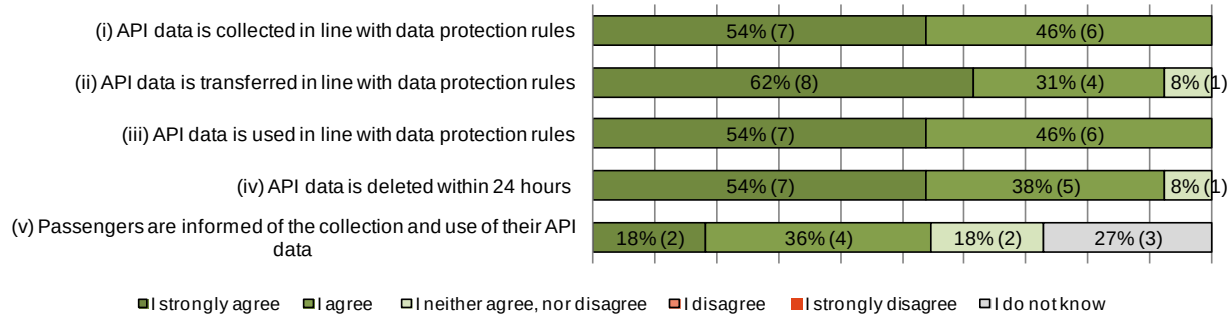
[207] RO

beforehand. The data is properly secured, and automatically deleted within 24 hours[208].

- Only one DPA did report cases of infringements related to fundamental rights.
  - In Estonia, there have been instances of data protection breach;
  - No complaints have been filed against carriers in relation to the collection and transmission of API data in other Member States[209];
  - There have been complaints on collecting personal data by two carriers relating to the amount of API data fields required;
  - A few air carriers have asked the Member States confirmation that the collection of API data by the competent authorities is in accordance with the law[210].

Figure 7.9 illustrates the extent to which competent authorities perceive national API systems to comply with data protection legislation. As illustrated, none of the thirteen responding competent authorities stated that their API system is in breach of data protection legislation

Figure 7.9 Competent authority perceptions of the extent to which national API systems are in line with data protection legislation (*n = 13*)[211]



Source: Competent authority responses to the following question in an online survey: Please comment on the following statements: (i) API data is collected in line with data protection rules, (ii) API data is transferred in line with data protection rules (iii) API data is used in line with data protection rules (iv) API data is deleted within 24 hours (v) Passengers are informed of the collection and use of their API data

Out of thirteen responding competent authorities only one reported that the processing of API data ever fails to meet overall data protection requirements.[212] Eleven other respondents reported that this never occurs and one provided no response.

[208] FI, PT

[209] AT, EE, FR, HU and UK

[210] DE

[211] Responses received from competent authorities in the following implementing countries: ES, AT, CZ, EE, CY, RO, IT, HU, CH, IE, DE, NL, MT

[212] This was reported by **Czech Republic** to occur around once every six months. Competent Authorities were responding to the following question: How often, on average, do you come across the following issues: (i) Data transmitted by carriers is not being used, (ii) The processing of API data does not meet the overall data protection requirements (iii) Adequate measures are not in place to inform travellers of the collection and use of their data.

7.3 Efficiency

Efficiency refers to the extent to which the functioning of the directive has achieved its objectives at a reasonable cost. This section provides findings with respect to the efficiency of the implementation of the Directive, in order to achieve the intended impacts.

The following assessments, as required by the Terms of Reference, have been made:

- The costs related to the practical implementation of API systems for Member States' carriers
- The operating costs of running API systems for Member States authorities and carriers
- The number of passengers affected by the API Directive since the implementation of the Directive

The above has been assessed with respect to the cost efficiency of implementing API systems for the national competent authorities (section 7.3.1.1) and air carriers (section 7.1.3.2). The overall efficiency of the Directive is also examined together with the number of passengers concerned by the Directive (section 7.1.3.3).

7.3.1 Costs of implementing API systems

The costs that have occurred from implementing API are varied. The costs are dependent on several factors such as, the type of system implemented and its functionalities, the number of routes for which API is implemented, the type of checks, assessment and analyses undertaken on API data and the API system's integration with other existing border management systems. Therefore, there is not just one cost model that would be applicable across the EU/EEA. The overall costs and cost effectiveness are dependent on the types of systems implemented. In line with this, the assessment of efficiency draws on data and information provided by the Member States implementing API, taking into account the differences between their systems, and highlighting the range of API related costs through specific examples.

7.3.1.1 Cost efficiency of API to national competent authorities

The cost to national competent authorities is dependent on the type of system implemented. They have either had to or decided to upgrade their existing systems to receive and process API data or keep the existing systems already in place. This has primarily been based on the level on need to upgrade already existing systems and on decisions regarding extent to which request and use the API data and the level and types of analysis to undertaken with the API data.

Table 7.7 provides an overview of total API system costs for a sample of national authorities implementing API systems. There is considerable variation across the Member States. This is partly explained by the cost items included in the total costs but also the type of system and the extent of the system implemented. For example, the costs for Switzerland are high because the reported costs cover the infrastructure and personnel costs in addition to equipment and communication costs. In addition, at a system level, the Swiss authorities have made an investment in an automated system that is fully operational in mid- 2012. Until then manual data checking had been performed on the basis of spot checks. In comparison, the costs for Austria are low as they currently operate a pilot system in the Vienna airport, and the reported costs cover only the API application costs, operational application costs and communication costs.

The focus of the table below is to illustrate the range of costs incurred by the competent authorities, with the knowledge that these reflect the different circumstances of the Member States.

Table 7.7 Overview of the total API operating system costs for national authorities

Country	2009	2010	2011	Cost items included	System characteristics
AT	€20,372	€8,988	€8,988	Dedicated API applications costs; Communications & maintenance; Operational applications	Austria's operates a pilot system (launched in 2010) which currently operates out of Vienna Airport only. This explains the comparatively low cost
DE	€277,764	€850,088	€771,000	General Operating & IT equipment costs; Communications & maintenance	Germany launched its API system in 2008, operating on specific air routes only. Germany undertakes statistical risk analysis on API data and implements automated system but also receives API data through non-automated means
RO	€2,500	€16,569	€17,135	General building & infrastructure costs (for 2009 only); Dedicated API applications costs; Communications & maintenance	Operational since 2009. Automatic system but also receives API on non-automated means. Undertakes risk analysis on suspected routes
CH			€ 2,497,743	General building & infrastructure costs; General Operating & IT equipment costs; Dedicated API applications costs; Personnel; Communications & maintenance; Operational applications	System is Switzerland is operation since mid-2012. It is automated, technically advanced, and replaces manual spot checks on API data
IT	€4,000,000		€4,900,000	*Not fully specified*	Italy has implemented (in 2011) a highly technologically advanced automated system where the authority accesses the carrier's online system to collect the data. API data is collected on targeted routes only. API is used for intelligence and future risk profiling

Source: National competent authority data submissions

The above costs can also be contrasted with API system costs using other models for implementation. For example, in comparison to the system costs elaborated above, the UK system (e-Borders) is an all-encompassing system, in which the API data stream forms a small part. For such a large border control system (incorporating several data flows), the costs of implementation has been estimated at €175 million by the competent authority, with the cost of first year of operation approximately at €20 million. In the case of Netherlands that currently makes use of a rental operating system and software, the costs for the data provider are approximately €110,000, and the software costs are approximately €250,000 per annum. For an API systems relying on private sector providers (i.e. SITA/ARINC) to

compile and aggregate the data the cost depends on the volume of data transmitted, and can range from less than €0.5 million to €10 million[213].

Greece and Poland have estimated implementation costs API for the systems that are due to be implemented in the near future. Greece has estimated the fixed cost for API at €250,000 over three years and the running costs at €150,000 per annum. The border guard in Poland estimated that the set-up costs would be in the order of €139,000[214]. These costs would include the financing of internet server and software (ca. €12,000), providing safe connection between the internet and the border control systems intranet (€7,000) and transferring API into the border management's operating system ODPRAWA (€120,000). In addition, the system is expected to cost approximately additional €8,000 per annum from providing safe connection for API data and translating API to XML format). The actual costs are likely to be higher as the costs indicated refer to the operational implementation costs regarding the IT and communications infrastructure only.

Overall, from the perspective of the level of financial investment by national competent authorities currently implementing API systems, the systems have not had a large impact on the relevant department's operating budgets. In six Member States implementing API systems, less than one per cent of the competent authority department's annual budget goes onto implementing the API system[215], and in the case of two Member States this was between one and five per cent[216]. Of these eight Member States, four had not experience any change in their department's annual budget[217], whereas in three Member States this had led to less than 1% increase in their annual budget[218] . In one Member State (Italy) API system costs had led to over 10% increase in the annual budget. This is perhaps expected given the comparatively high cost of the API system in Italy.

7.3.1.2 Cost efficiency of API to air carriers

Most industry stakeholders expressed their concerns about the implications of the API Directive in terms of compliance costs for air carriers. The basis of their concern was that the industry is required to implement a system which is focussed on meeting the States' security objectives but which generally does not bring any benefits to the carriers. The costs of implementing API systems relate to both upfront technological costs and to operational resources (i.e. staff in charge of operations, institutional relations, development and maintenance of the API systems). The general perception has been that API system diverts airlines internal resources from carrying out commercial activities and providing best in class services to passengers. The text box below provides an example of the main cost drivers for major EU/EEA national flag carriers. The example presented implies a major integrated system, and some smaller carriers are unlikely to implement systems and procedures with such high sophistication. The carriers specified that their reasons to invest in API system relate to the obligation to provide API and it is in the carriers' interest to invest in time-efficient methods of collecting and transmitting data (i.e. by investing in passport readers (hardware) and software, rather than the staff and time costs of collecting and transmitting this manually.

Example of cost drivers for major EU / EEA air carriers

Given that the major carriers provide API services for 10-20 countries, the set-up costs stemming from the EU Directive's obligation are somewhat reduced, since the systems were already in place. In addition, as API has been integrated into the entire operating systems (e.g. online booking,

[213] One stakeholder reported the cost of such system to be approximately €100,000 a month or €1.2 million a year for a relatively small Member States with relatively limited international air traffic. Some carriers have indicated the cost of such system to be approximately €0.5 million.

[214] The figure reported by the Border Guard was 580,000PLN which was converted into Euros using the XE universal currency converter, with the exchange rate of 1PLN to 0.237498EUR

[215] AT, EE, RO, HU, IE and DE

[216] IT and CY

[217] IE, RO, EE and CY

[218] DE, HU, AT

frequent flyer services, passport-checking facilities, etc), the costs cannot always be easily isolated. The main implications of the API requirement can be summarised as follows:

- in consideration of the **operational costs** of transmission and of storage and archiving API systems alone costs around 0.5 – 1 million euro per year
- extra **set-up costs** are incurred– e.g. (i) when carriers start operating in a new airport, as they will need to invest in passport readers to comply with API requirements; (ii) when they create new online services
- other costs include **training costs** (API system training is now built into all general training systems
- **contingency costs –** i.e. back-up systems to ensure that API can still be collected even if the original system breaks down
- **staff costs –** there is a dedicated IT team responsible for monitoring API systems in an IT centre. The staff costs associated to API systems in Europe are around 100,000 euro. It should be noted that the processing of API for carrier crew is more complicated and requires some different processing than passenger API.

Overall, the API Directive related compliance costs for carriers range from less than €0.5 million to over €2 million on average per carrier per annum after the set-up costs have been absorbed[219]. The range of costs for carriers in five Member States is presented in Table 7.8 below. As a broad generalisation, it seems that costs for major carriers are in excess of €2 million, whereas for smaller carriers these costs would be around €0.5 million or less, depending on the number of flight routes from third countries for which API is collected.

Table 7.8 Overview of air carriers API system costs

Carrier	Estimated set-up and operating costs[220]	Estimated annual operating cost[221]
Carrier 1 (smaller EU carrier).	Less than 0.5 million euro	Less than 0.5 million euro
Carrier 2 (smaller EU carrier)	Less than 0.5 million euro	Less than 0.5 million euro
Carrier 3 (medium size EU carrier)	Less than 0.5 million euro	0.5-0.99 million euro
Carrier 4 (Major EU carrier)	*Not indicated*	2 million or over 2 million euro
Carrier 5 (EEA carrier)	*0.5-0.99 million euro*	Less than 0.5 million euro

Source: Air carrier responses to the following two questions in an online survey: Please estimate your API related set-up cost relating to the EU Directive, including (i) general operating and IT equipment cost and (ii) dedicated API application costs and Please estimate your API related operating costs per annum, including personnel, communication & maintenance and operational application costs

An estimated, typical, cost breakdown of API is provided in the Table 7.9 below, together with a comparison against PNR costs, as was established in the impact assessment undertaken on PNR. However, the cost ranges are likely to be variable, depending on the

[219] This is based on information provided by eight carriers consulted in this study, six of which provided a response to the online industry survey.

[220] This includes (i) general operating and IT equipment cost and (ii) dedicated API application costs

[221] This includes API related operating costs per annum, including personnel, communication & maintenance and operational application costs

system requirements and the API specific requirements, including the extent of the data collection and transmission. Table 7.10 further estimates the specific on-going cost drivers of complying with the Directive, such as the development costs per additional route and the transmission / communication costs per passenger.

Table 7.9 Estimated costs for setting up API systems for air carriers and for one year of operation

Cost driver	Estimates from IA on PNR Proposal (2011)	Estimates from Interviews (2012)
Set-up costs (pull system)	*€400,000*	€450,000 on average[222]
Set-up costs (push system)	€1,200,000	
Transmission costs (using push) – only on inbound flights to EU	€ 116,000	N/A
Personnel cost (operation)	€400,000	€100,000[223]
Personnel cost (Training and maintenance)	€160,000	N/A
Total set up costs (push system)	**€1,200,000**	N/A
Total Operating costs [224]	**€676,000**	**From €500,000 to €1,000,000**

Source: Proposal Directive on PNR on the basis of information provided by carriers, ICF GHK interviews and ICF GHK calculations

Table 7.10 Estimated itemised costs of compliance

Cost driver	Estimates from IA on PNR Proposal (2011)	Estimates from Interviews (2012)
Development costs per additional route	*N/A*	€10,000 to €15,000
Development costs per change request	*N/A*	€50,000[225]
Transmission / communication costs per passenger	From €0.03 to €0.04[226]	€0.38 to €0.4[227]

Source: Proposal Directive on PNR on the basis of information provided by air carriers, ICF GHK interviews and ICF GHK calculations

In addition to system related costs, with respect to data collection and transmission, carriers can also be imposed costs on the basis of non-compliance. This is the form of a loss of revenue from the business operations through imposed sanctions.

Over €1.7 million in fines have been imposed on carriers over the evaluation period. The actual number is likely to be higher, as there is a chance that not all information has been possible to submit to the evaluators. The table below reports on the volume and corresponding amounts of sanctions imposed on carriers relating to those Member States that we able to provide the information.

[222] The cost can range from €50,000 for a single PC-based solution to €8,000,000 for a distributed control system.

[223] Cost of staff for operating API systems in Europe only.

[224] Note that these are PNR system related cost. However, few air carriers confirmed the range of operating cost for an API system as being between €0.5 million to €1 million per year, i.e. broadly in the same range.

[225] Typically include 200 man-hours (at €77 per hour), scoping study, evaluation of impact on legacy systems, development of the solution, programming and test of the solution.

[226] Communication costs only

[227] Includes transmission costs, collection and transformation but excludes software and system costs.

Table 7.11 Volume and cost of sanctions imposed on air carriers over the 2006-2011 period

Member State	Number of sanctions	Total amount	Average amount by sanction
AT	154	€936,000	€6,078
CZ	N/A	€ 37,000[228]	-
HU	≤ 4[229]	≤ €12,000	€3,000
LV	≤ 4[230]	≤ €12,400	€3,100
RO	7[231]	€20,835	€2,976[232]
DE	N/A	688,233	-
Total	Est. ≤ 181	≤ €1.70 million	€5,624

Source: Data submission from national competent authorities and ICF GHK calculations.

The bases on which these sanctions have been imposed have been reported in sections 6.6.2 and 6.7.

7.3.2 The overall efficiency of the Directive and the number of passengers concerned by the API directive and

The numbers of international passengers that are subject to API requirements vary across the Member States. Some Member States collect data on all non-EU flights (e.g. EE, CY, RO, IE and ES), whereas other Member States have a more targeted approach by requesting API on certain routes, which are considered risky (e.g. AT, DE, CZ, HU, CH, NL and MT). For example, Switzerland and Malta collect data on less than 10% of international passengers, though it is important to note that these countries have only recently started implementing API. Table 7.12 below indicates the proportion of international passengers for whom API is collected.

Table 7.12 Overview of the proportion of international passengers whose API is collected

	Less than 10%	11-20%	21-30%	31-40%	41-50%	51-75%	75-100
Member State	CH, IE, MT	HU	n/a	NL	AT	CZ	EE and RO

Source: Competent authority responses to the following two questions in an online survey: What is the proportion of international passengers arriving into your country for which API data is collected?

It is also clear that the numbers of passengers affected by API collection varies in the different Member States, given the volume of international passengers arriving in these countries. This is also an impact factor on the costs arising from the implementing of API systems. Given the resources and main objectives, it may not be desirable to collect API on all international passengers. Table 7.13 below provides an overview from some Member States implementing API regarding the actual volume of the API data collection.

Moreover, the overall efficiency with respect to outcomes of the API data collection is difficult to measure. Some indication of this is available from Germany. Their data indicates the

[228] 2011 only

[229] Fines have been imposed on the following carriers: MALEV, Aeroflot, Turkish Airlines and Egypt Air.

[230] Three in 2008 and one in 2011. In 2011, four sanctions were dropped after a complaint by carriers to a competent authority dealing with complains.

[231] In 2010, a total of 50 000 RON (11,120 EUR) have been imposed following 4 cases of breach (three amounting to 10.000 RON and one amounting 20.000 RON). In 2011, a total of 40 000 RON (8,896 EUR) have been imposed following three cases of breach (two amounting to 10.000 RON and one amounting to 20.000 RON)

[232] Note that the average does not correspond to the minimum sanction of €3,000 as specified in the Directive. However, this could be a question of exchange rate variations as December 2010 and December 2011 exchange rates were used to perform the calculations.

number of flights subject to API data collection, and the number of persons that were wanted or recognised by the system traveling on those flights. This data provides some indication of the overall efficiency, though it is an approximate. It can be estimated that over the past four years (2008-2011) API used has provided a match for a wanted person in about 7% of all the flights subject to API data collection. In other words, one in every fourteen flights has carried a person that has been wanted by the authorities or recognised by the border control systems, and the API data has been useful for these purposes. Table 7.14 below indicates the number of flights subject to data collection and the number of persons wanted or recognised from those flights.

Table 7.13 International passengers concerned by API requirement (2009-2011)

	Austria			Italy			Romania			Spain[233]		
	2009	2010	2011	2009	2010	2011	2009	2010	2011	2009	2010	2011
Overall international air passenger arrivals	4,102,776	4,400,298	4,643,622	(-)	(-)	16,466,509	105,111	363,410	403,950	12,016,658	14,772,325	17,402,084
Passengers who API is collected	unknown	9,49,468	1,988,135	(-)	(-)	12,91,805	105,111	363,410	403,950	8,113,868	11,171,521	14,129,166
%	n/a	22%	43%	(-)	(-)	10%	100%	100%	100%	68%	76%	81%

Table 7.14 Indication of the efficiency of API in Germany – number of persons identified through API and the proportion of flights this applies

	2008	2009	2010	2011	Total
Total number of flights where API data have been transmitted	8460	26889	44587	59139	139,075
Number of persons who were wanted and recognized by the system	706	1652	3112	4121	9,591
Approximate proportion of all flights for which wanted person recognised[234]	8%	6%	7%	7%	7%
Rate of inspection in terms of flights for which wanted persons recognised[235]	1 in 12	1 in 16	1 in 14	1 in 14	1 in 14

[233] The data for Spain has been calculated using a proxy. For all international passenger arrivals, the proportion of flights for which API is collected is used to approximate the number of persons subject to API data collection. In practice it seems that Spain collects API on all non-EU flights (survey response).

[234] GHK calculation: This is an approximate as it assumes one person is recognised per flight. In reality there may be more than one person that is recognised within the same flight.

[235] GHK calculation: This is an approximate as it assumes one person is recognised per flight. In reality there may be more than one person that is recognised within the same flight.

Overall assessment of cost efficiency is challenging due to the lack of systematic data that could be used for the assessment. From the competent authorities' perspective, the API systems have had an impact at a reasonable cost. None of the authorities thought that API was not cost efficient at all, but the perceptions of overall efficiency ranged from very low to very high. This is indicated in Table 7.15 below.

Table 7.15 Overall cost efficiency of API system with respect to outcomes

Very high	High	Medium	Low	Very low
IE	EE and CY	AT,CZ, IT, HU, DE	CH	RO

Source: Competent authority responses to the following question in an online survey: How would you rate the overall efficiency of the API system in your country with respect to achieved outcomes?

However, it has not been possible to directly qualify these judgements by outcome data and make direct comparisons between the costs and impacts. This may also not be advisable as many on the Member States only recently implemented the API system, or are still running a pilot system, which would not make a fair comparison. For example, Switzerland operated a manual system until mid-2012 and until the system is fully operational the full benefits cannot be realised. It is also yet uncertain what the full benefits will be, given that the technical functionality of the system is operational from the latter part of 2012. This is also partly the reason why specific and systematic outcome data is not available in many of the Member States. The main conclusions regarding the overall efficiency relate to the following measureable factors, available in few Member States:

- Over the past two years (2010-2011) in Austria, action has been taken against 0.4% of all international passengers whose API data had been collected;
- In the past year (2011) Italy, action has been taken against 0.7% of all international passengers whose API data had been collected;
- Over the past four years (2008-2011) in Germany, in approximately 7% of flights for which API data had been collected a wanted person was recognised by the system, which means that on average 1 in 14 flights a match is made to a wanted person / person subject to an alert

From the perspective of the carriers the Directive has not been considered cost efficient as it has not improved timeliness of flights or general carrier security. It has also diverted carriers from undertaking core business activities to dealing with API data and has brought costly changes to customer practice relating to collection and transmission of additional information.

The overall impacts are elaborated in section 7.4.

7.3.3 Other elements for judging the cost effectiveness of the Directive

Other elements that could be used for judging of the cost efficiency of the Directive include administrative costs. These mainly refer to (1) costs for Data Protection Authorities and (2) costs administrative proceedings (i.e. including sanctions).

Is has not been possible, nor required by the study, to directly collect these indirect costs arising from the implementation of API. However, some indication can be provided on the basis of the Impact Assessment of the PNR Directive. It estimated that on average the cost inspecting and checking of PNR system is €2.71 million on average[236]. Similar cost items for API system are likely to be in the same order of magnitude.

As to the administrative costs regarding sanctions, to date there have been at least 181 sanctions in total imposed on European Air carriers totalling a minimum of €1.70 million. This

[236] This would typically include cost of the vetting process, managing authorisations, inspection by DPAs, etc.

does not take account of court costs. If these are taken into account the overall cost of standing in tribunal could amount to €834,000[237].

7.3.4 Obstacles encountered in achieving the objectives of the Directive in a cost-efficient manner

Overall, the obstacles encountered in achieving the objectives of the Directive in a cost-efficient manner mainly relate to:

- The costs of implementation for national authorities and carriers: A balance has had to be struck between the technical and analytical sophistication of the API systems, the volume and routes for API data collection, the expected risks to be averted and the expectations on the types of outcomes achieved and
- The gradual implementation of API systems, partially through pilots, for which the full intended benefits have not yet been achieved and to an extent cannot be measured;

7.4 Impact

This section provides findings with respect to the impact of the Directive.

The impacts, i.e. end results of the Directive signifying change to situation prior to the Directive's implementation, are difficult to directly attribute to the Directive. This is in particular as border management systems are integrated, and the use of several data streams at once is the norm. API forms a part of these data streams, and systems that are used in conjunction with each other. Therefore, as far as possible, this is taken into account and elaborated in the relevant parts of the analysis[238].

The assessment in this section focuses on impacts on border control and law enforcement authorities as well as impacts on carriers, airport authorities and passengers, including impacts on third countries. More specifically, the following impacts are being assessed:

- Impacts on border control, such as on border management procedures, technological innovation and number of persons undergoing second line checks and/or being refused entry;
- Impacts on law enforcement authorities, such as extent to which data has been used for law enforcement purposes, in what proportion of instances and for which specific purposes;
- Impacts on carriers and their industries, including for cruise line companies and air/rail traffic in Member States where API is implemented to this effect;
- Impacts on passengers and airport authorities; and
- Impacts in third countries.

7.4.1 Impact on border control and border management

The main impacts of the Directive include better border controls and increased ability to combat illegal immigration. In some Member States there has been an improvement in the border control and checking procedures. The API Directive has also had some impact on technological innovation regarding the border management systems.

As a consequence of the API systems, the border management authorities have become better prepared for their general border control activities and in combating illegal immigration. Overall, the implementation of API has helped to improve border controls, as data has been received in advance, providing additional preparatory time and an ability to target in advance passengers who are subject to an 'alert'. This has been made possible

[237] Based on GHK calculation and Council of Europe Efficiency and quality of Justice Edition 2011 (data from 2008) – Calculated by taking the median of court cost over the EU27 (Median=€4607 per court case).

[238] In the data collection phase the stakeholders were specifically asked impacts relating to API, and impacts realised as a result of the API.

through advance information indicating suspect persons being among the passengers, providing additional time to react according the alert and risk analyses. Moreover, the level of scrutiny of this task has been reinforced with the prior automated checks and subsequent detailed checks that are being carried out.

In these respects API systems have also facilitated identification of suspect passengers. Example of this in Germany is shown in the text box.

Impact of API on improved border control in Germany

Prior to the implementation of the Directive it was difficult to obtain the names and travel routes of certain type of migrants who destroyed their travel documents in order to hinder their identification. The authorities in Germany had observed this phenomenon for years, and consequently were aware of the routes. The introduction of API has enabled the targeting of such migrants and subsequently their identification of the basis of API, which was further enabled because of the obligation in Germany of air carriers to also transmit the flight route.

Overall, the competent authorities had a positive perception with respect to the impact of the collection and use of API data in terms of the faster reaction it enabled against suspect illegal migrants and suspect criminals. Over 60% of competent authorities considered that API data had a very large or considerable impact in these respects. The main perceptions are summarised in below.

Table 7.16 Perception of the impact of API with respect to faster reaction against suspect illegal migrants and suspect criminals (*5 = very large impact; 0 = no impact)*[239]

	5	4	3	2	1	0
Faster reaction against suspect illegal migrants	3 (27%)	4 (36%)	2 (18%)	1 (9%)	0 (0%)	1 (9%)
Faster reaction against suspect criminals	3 (25%)	5 (42%)	1 (8%)	1 (8%)	0 (0%)	2 (17%)

Source: Competent authority responses to the following question in an online survey: Please rate the direct impact of the collection and use of API data in your country with respect to the following impacts on border control: (i) Faster reaction against suspect illegal migrants, (ii) Faster reaction against suspect criminals

The border procedures have also improved in the case of certain Member States whereby the second line checks are clearer. For example, in the case of Czech Republic both the border police and border control staff focused on suspect passengers arriving at the border checking points, based on the API data that had been transmitted by the carriers in advance. More specifically, API data has helped to identify suspected persons, and for example, in in 2010, 91 suspect persons were detained in Czech Republic, 68 of which were done on the basis of the API data.

API systems have had some impact on technological innovation. Although new systems created for border management in certain Member States (e.g. in the Czech Republic) are based on good functionality, the connection to SITA however, uses an old format from the sixties. The introduction of API system has in some cases also led to an upgrade of databases in the border management authority, which has been the case in Romania for example. Overall, the competent authorities had a positive perception of the impact of API on faster border checks and increased technological innovation, although this was not as clearly marked as the perceived impact on faster reaction against suspect illegal migrants and suspect criminals. Table 7.17 provides an overview of the level of the impacts.

.

[239] This is based on respondents from 11 to12 Member States that are currently implementing API and responded to the relevant question in the online survey.

Table 7.17 Perception of the impact of API on speed of border checks and increased technological innovation (*5 = very large impact; 0 = no impact*)[240]

	5	4	3	2	1	0
Faster border checks	2 (18%)	2 (18%)	0 (0%)	3 (27%)	2 (18%)	2 (18%)
Increased technological innovation	1 (9%)	4 (36%)	2 (18%)	1 (9%)	2 (18%)	1 (9%)

Source: Competent authority responses to the following question in an online survey: Please rate the direct impact of the collection and use of API data in your country with respect to the following impacts on border control: (i) Faster border checks*, (ii)* Increased technological innovation

7.4.2 Impact on combating illegal immigration and impact on law enforcement

Although the impacts of the API data on illegal immigration and law enforcement are difficult to measure, particularly as authorities tend not to keep records of number of cases and purposes for which API data has been used, the authorities stipulated the types of impacts deriving from the implementation of API systems.

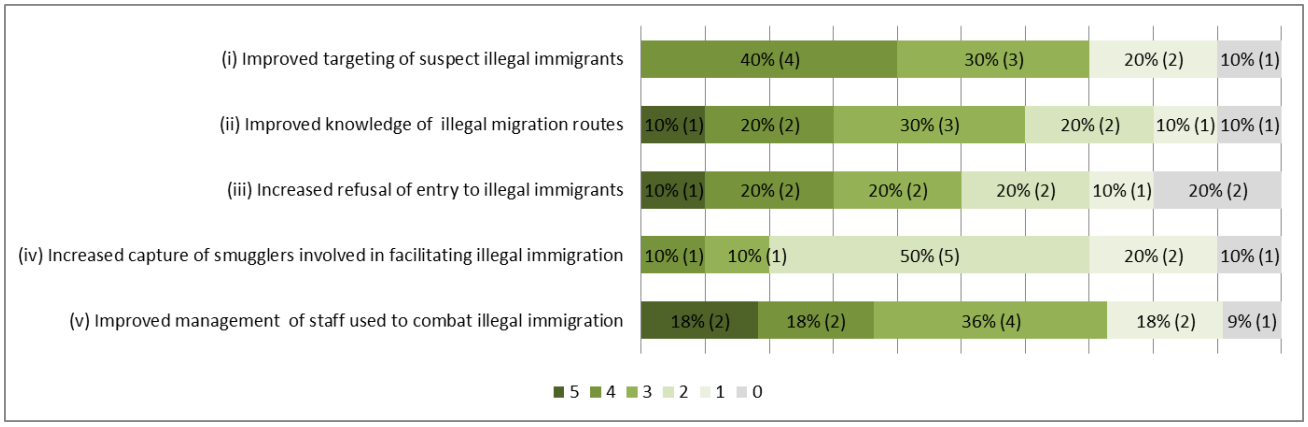
API systems have had a clear impact on combating legal immigration, improved internal security and to some extent API systems have contributed to capturing criminals. In particular, the competent authorities perceived that API systems contributed to the management of staff used to combat illegal immigration and helped targeting of suspect illegal immigrants. API systems also had an impact on improved knowledge of migration routes and to an extent had increased refusal of entry to illegal immigrants. One of the main impacts on improved internal security included better risk profiling and carrying out risk analysis to identify suspected persons, including criminals. API had very little or no impact with respect to collaboration with other countries regarding law enforcement efforts. API was perceived to have some impact in increase in the arrest of criminals in five Member States. In addition, in Belgium, France and United Kingdom, stakeholders used or consider API data as relevant for custom enforcement purposes (e.g. import or export of drugs).

The competent authorities perceived that API systems contributed to the management of staff used to combat illegal immigration and targeting of suspect illegal immigrants. API systems also had an impact on improved knowledge of migration routes and to an extent had increased refusal of entry to illegal immigrants, whereas the use of API data have had very little impact on the detection of smugglers involved in facilitating illegal immigration. The Figure 7.10 below presents the overall level of API systems' impact on combating illegal immigration, where 5 indicates a 'very high level of impact' and 0 indicates 'no impact'[241].

[240] This is based on respondents from 11 Member States that are currently implementing API and responded to the relevant question in the online survey.

[241] This is based on responses from 11-10 competent authorities in Member States currently implementing API.

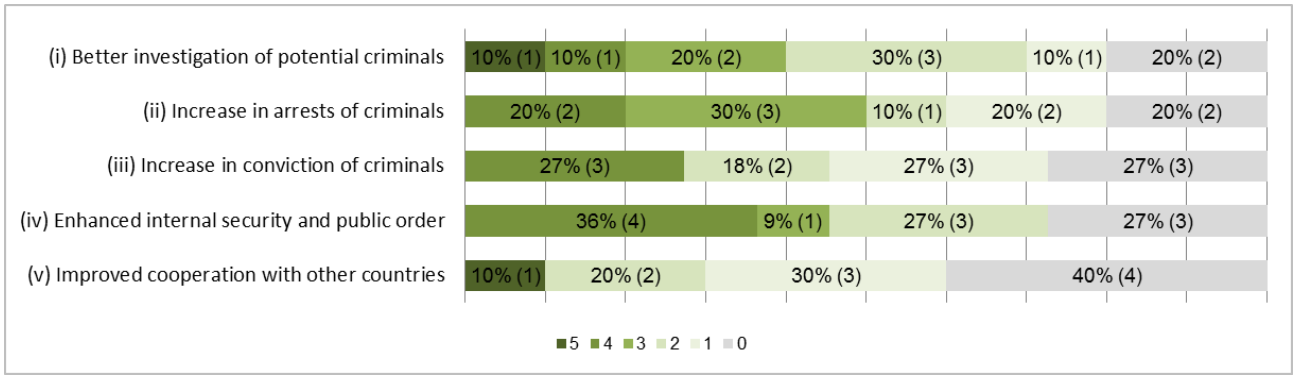
Figure 7.10 The impact of the collection and use of API data to combating illegal immigration



*Source: Competent authority responses to the following question in an online survey: Please rate the direct impact of the collection and use of API data in your country with respect to the following impacts on combating illegal immigration (*5 indicates a 'very high level of impact' and 0 indicates 'no impact')

The impact on API data collection and use of API data on law enforcement purposes was not perceived to be as large as the impact on fighting illegal immigration. However, the most considerable impact in this respect related to an enhanced internal security and public order. The collection and use of API had very little of no impact with respect to collaboration with other countries regarding law enforcement efforts. The use of API data was perceived to have some impact in increase in the arrest of criminals in five Member States, whereas in three Member States it had also contributed to the increase in conviction of criminals. The impact of collection and use of API data on several aspects relating to law enforcement is indicated in in Figure 7.11 below[242].

Figure 7.11 The impact of the collection and us of API data to law enforcement purposes



*Source: Competent authority responses to the following question in an online survey: Please rate the direct impact of the collection and use of API data in your country with respect to the following impacts on law enforcement (*5 indicates a 'very high level of impact' and 0 indicates 'no impact')

A few stakeholders commented on the scale of these impacts for border control and law enforcement authorities as a result of the use of API data. This is shown in Table 7.18 below.[243] Overall, a majority of competent authorities considered that API data had little impact on persons being detained for "national security" reasons. Only one Member State stated this reason with on average, one person in 10,000-20,000 being detained for this reason. In two Member States an alert is being sent to border control authorities in other Member States with the frequency of one in every 10,000-20,000 persons. In three Member States one in 10,000-20,000 persons is refused entry at the border and in two Member States one in 10,000-20,000 person is arrested at the border for a suspected crime.

[242] This is based on responses from 11-10 competent authorities in Member States currently implementing API.

[243] This is based on responses from 8-10 competent authorities in Member States currently implementing API.

Table 7.18 Perception of the impacts on border control and law enforcement as a result from the use of API[244]

	No impact	One in 10,000-20,000	One in 21,000-30,000	No records
Person refused entry at the border	2 (25%)	3 (38%)	1 (13%)	2 (25%)
Person arrested at the border for a suspect crime	3 (38%)	2 (25%)	1 (13%)	2 (25%)
Person detained due to national security threat	4 (57%)	1 (14%)	0 (0%)	2 (29%)
Alert sent to authorities in other Member States	5 (50%)	2 (20%)	0 (0%)	3 (30%)

Source: Competent authority responses to the following question in an online survey: Please comment on the impacts of border control and law enforcement as a result of the use of API data. Please indicate the scale of occurrence with respect to the following

In addition to the above estimates, further evidence of actual impacts and their scale is available only in a sample a Member States. Even though no systematic comparable evidence is available across all the Member States, the following can be evidenced:

- Over the past two years (2010-2011) Austria recorded 12,332 cases where API data had been used by the border management authorities to take action against international passengers. Five of these cases concerned detaining a person at the border as a result of use of API data. Compared to the number of international passengers whose API data was collected during the same period, action has been taken against 0.4% of all international passengers whose API data had been collected[245].
- In the past year (2011) Italy recorded 85,222 cases where API data had been used by the border management authorities to take action against international passengers. Of these, 326 persons were refused entry at the border and 34 detained at the border. Compared to the number of international passengers whose API data was collected during the same period, action has been taken against 0.7% of all international passengers whose API data had been collected[246].
- In the past four years (2008-2011) 2,322 persons have been refused entry at the UK border as a result of API data used by the border control authorities. No complete data is available to calculate the total number of cases for which API was used. Evidence regarding the UK system (of which API form a part) also implicates that Semaphore captured data on 47 million passenger movements and issued over 20,000 alerts to border agencies, resulting in more than 1,800 arrests and other interventions for crimes, which also made a significant contribution to countering terrorism[247].
- In the past six years (2005-2011), in the UK as a part of operation to counter human trafficking and smuggling, 17,000 persons have been returned to third countries as a result of the monitoring of API and 27 facilitators have been arrested. In addition, 240 lost/stolen passports/documents have been seized[248].

[244] This is based on respondents from 8 to10 Member States that are currently implementing API and responded to the relevant question in the online survey.

[245] This has been calculated on the basis of number of passengers whose API data was collected during the same period.

[246] This has been calculated on the basis of number of passengers whose API data was collected during the same period.

[247] Tom Dodd, Director, Border and Visa Policy, Minutes of Evidence, Further supplementary evidence by the Home Office, 6 May 2008.

[248] The statistics are based on information provided during the interview with the UK Border Management Authority.

7.4.3 Impact on carriers

This section provides an assessment of impacts of the implementation of the API Directive on air carriers. It has not been possible to determine impacts on other types of carriers, as in those countries where API system is implemented, API data collection and transmission primarily relates to air carriers.

The main impact on air carries concern the costs of implementing the API system, the API Directive's impact on changes to business processes and sanctions that have been imposed on the basis of incorrect, incomplete or non-transmitted data.

There is a strong perception amongst the air carriers that they absorb the cost of implementing the Directive, without receiving direct business benefits. According to the airlines consulted, national authorities' requirements are considered as a matter of priority within the airline which diverts resources and time from carrying out commercial activities. The added issue for the air carriers is that the API system is regulated differently in different Member States, which requires that air carriers ensure the API transmission matches to those requirements. According to one airline, cost estimate can be to up to tens of millions of Euros per year. The main cost drivers identified include:

- Non-harmonised, redundant and incompatible requirements from authorities worldwide
- Data quality issues for which airlines are held responsible
- Large IT development costs and processing time at stations for airlines: such a system requires specific IT development and training
- Operating costs, which are high due to the high level of data transmitted

In addition, in some Member States, such as in Germany, carriers could not use their existing system, which resulted in higher administrative burden and costs. According to the air carriers they have had to spend about 10,000 to 15,000 Euro on new systems for each flight route where the API data are collected. In addition, air carriers are generally responsible for covering the data transmission costs where a third party system has been used to transmit data (e.g. SITA, ARINC).

Even where carriers had implemented API prior to the obligations stemming from the Directive, set-up costs have been incurred as the obligations are different. The level of cost also differs across the carriers, which dependent on the level of obligation and number of routes for which data is to be transmitted. Table 7.19 below provides an overview of the set-up and operating costs for sample of carriers that had implemented API prior to the Directive (with the exception of one carrier)[249].

Table 7.19 Overview of air carrier set-up and operating costs

Carrier	Estimated set-up cost[250]	Estimated annual operating cost[251]
Carrier 1 (smaller EU carrier).	Less than 0.5 million euro	Less than 0.5 million euro
Carrier 2 (smaller EU carrier)	Less than 0.5 million euro	Less than 0.5 million euro
Carrier 3 (medium size EU carrier)	Less than 0.5 million euro	0.5-0.99 million euro
Carrier 4 (Major	*Not indicated*	2 million or over 2 million euro

[249] These responses were provided by five carriers responding to the relevant question in the online industry survey.

[250] This includes (i) general operating and IT equipment cost and (ii) dedicated API application costs

[251] This includes API related operating costs per annum, including personnel, communication & maintenance and operational application costs

Carrier	Estimated set-up cost[250]	Estimated annual operating cost[251]
EU carrier)		
Carrier 5 (EEA carrier)	0.5-0.99 million euro	Less than 0.5 million euro

Source: Air carrier responses to the following two questions in an online survey: Please estimate your API related set-up cost relating to the EU Directive, including (i) general operating and IT equipment cost and (ii) dedicated API application costs and Please estimate your API related operating costs per annum, including personnel, communication & maintenance and operational application costs.

Three of the six carriers responding to the online survey had been subjected to sanctions, with a smaller EU carrier 1-5 times and a major EU carrier over 20 times. In all instances sanctions had been imposed on the grounds of faulty or incorrect data or a late transmission of data. However, this is not necessarily a reflection of carriers' compliance but the ability and willingness of authorities to impose sanctions, especially when a pilot system has been operated. Information from national competent authorities indicates that at least carriers in six of the 19 countries implementing API systems have been subjected to over 180 sanctions. Romania to date has had two court cases where the carrier has challenged the decision of the Border Police to impose sanctions.

Overall, the implementing of API system has led in some cases the airlines having to make changes to their business processes. For example, according to one airline the collection of API affects (i) timeliness of flights and (ii) customer practice as customers are required to provide additional information. The airline has had to adapt to these changes by changing their business process accordingly. Consequently the air carrier has (i) invested in automated systems with hardware and software and (ii) created systems for passengers to store API so that they are not required to re-enter it for each flight. For example, when API is entered into the system, the airline will store this for the life of the booking, so that there is no need to re-enter the API prior to the return leg of the journey. Frequent Flyers are also provided an option of entering their API data into an « executive club record » which is secure and adheres to data protection requirements. The data is stored and there is no need to re-enter it each time they fly to countries with API requirements. These changes have taken place so as to enable airlines to make their systems leaner and reduce the administrative burden stemming from the requirement to transmit API data.

Generally, the carriers also had a negative perception of the impacts of API systems. They were asked to comment on the impact of API on several grounds and state how strongly they agreed with or disagreed with the impact statements. The results were as follows:

- **Improved timeliness of flights**: four out of five carriers commenting the statement either disagreed or strongly disagreed that timeliness of flights had been improved
- **Improved general carrier security**: five out of six carriers commenting the statement either disagreed or strongly disagreed that API had improved general carrier security
- **Diverted carriers from undertaking core business activities to dealing with API data**: five out of six carriers commenting the statement either agreed or strongly agreed that API had diverted carriers from undertaken core business activities
- **Brought costly changes to customer practice relating to collection and transmission of additional information:** all six carriers commenting the statement either agreed or strongly agreed that API had brought costly changes to customer practice regarding collection and transmission of additional information
- **Brought positive changes to business processes relating to implementation of better technology**: five out of six carriers commenting the statement either disagreed or strongly disagreed that API had brought positive changes to business processes regarding implantation of better technology

The carriers were not sure whether the use of API had brought positive changes to customer practice relating to better facilitation of information: one carrier agreed, two disagreed and three did not have a firm opinion regarding this. However, two carriers indicated that API

data had deterred suspect persons from boarding the carrier, whereas one carrier did not know of this type of impact and three carriers disagreed that this had been the case.

Some of the carrier representatives also considered that air carriers were put at disadvantage when compared to non-air carriers that had not been required to adhere to the obligation to transmit API data.

When asked to rate the overall impact of API in the scale of +5 to -5 (*5 = very large positive impact; 0 = no impact; -5 = very large negative impact*), the carriers generally had a negative perception of the overall impact of API. Table 7.20 below presents the overall impact score and the main explanation to rating provided by carrier responding to the industry survey.

Table 7.20 Overview of the carriers' rating regarding the overall impact of the implementation of API system to carriers

Carrier	Impact rating	Explanation to rating
Smaller EU carrier	+3	*Not provided*
Smaller EU carrier	-1	The API system has not brought any positive results for our company corresponding to the investments made
Medium size EU carrier	-2	API has little value for the airlines. The costs must - sooner or later - be borne by the passengers.
Major EU carrier	-3	It is difficult to identify any benefit for both the airline and the passenger. Airlines are still facing improperly documented passengers (visa revoked for instance, fraudulent document), detected by the authorities of the country of destination upon the arrival process (and not prior departure). In addition, all passengers still need to go through lengthy immigration process (outside of Schengen).
Major EU carrier	-4	API causes delays, impedes processing time and design of procedures. It has an impact on IT development and operations. Training needs to be provided to staff, and error analysis undertaken on the data prior to transmission. Fines have been imposed and there has been revenue loss as a result of API. Communication costs and overheads have been increased and additional consulting costs incurred.
EEA carrier	-3	As passengers are able to enter their API data, the quality is not often very good. Given the possible sanctions, the carrier has had to introduce checks to verify that the API data is correct.

Source: Air carrier responses to the following question in an online survey: How would you rate the overall impact of the implementation of API system to carriers? 5 = very large positive impact; 0 = no impact; -5 = very large negative impact

7.4.4 Impacts on third countries and impacts on international relations

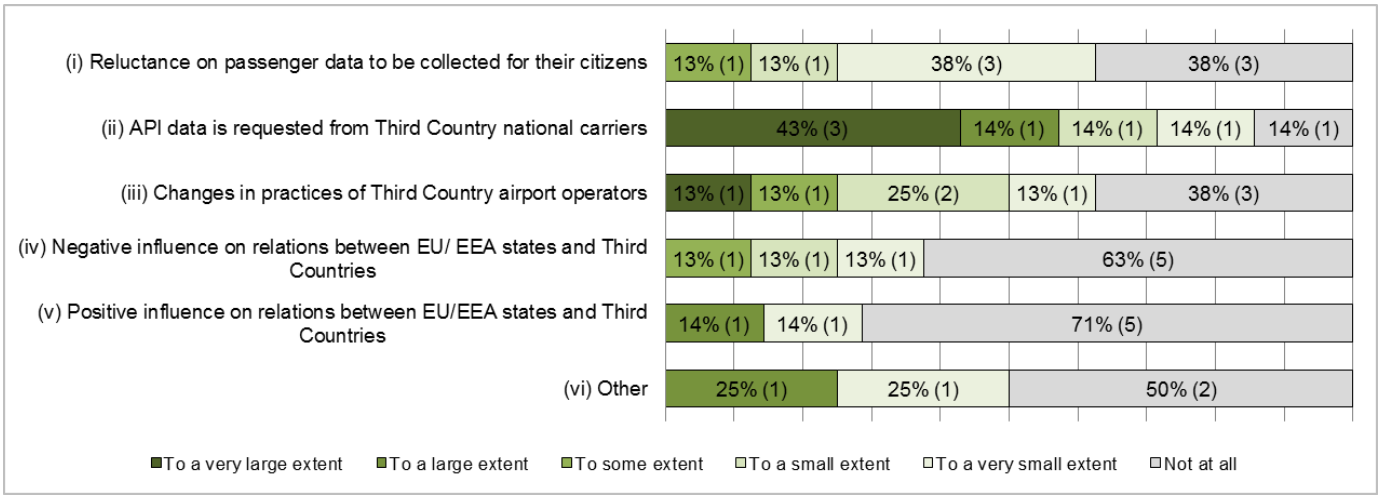
The impact of the Directive on third countries and on international relations appears relatively limited. This may be due to the fact the number of countries implementing API systems have increased over the period, i.e. including outside Europe and the USA. The relatively widespread nature of API systems and requirements may have facilitated the introduction of Member States' own systems with regard to third countries. Although third countries may have had some concerns about the use of API data from their citizens, only in a few instances data protection issues were mentioned by stakeholders:

- Few data protection issues affecting international relations have been identified, except perhaps in relation to the processing of API of EU citizens in third countries. The issue is that Member States' data protection systems tend to be more advanced compared to those of third countries

- One particular issue was reported by a German authority where a third country air carrier, affected by the obligation to transmit data, complained in their country of origin about EU API data requirements. The third country in question contacted the German authorities regarding the data requirement but were satisfied by the explanation that the same requirements would concern German carriers landing and departing from the given country airport.

Overall, the national competent authorities considered that there had been little impact on Third countries apart from that API data had been requested from third country carriers and there had been changes in practices of third country airport operators. Little impact was identified in relation to its influence on relations between the EU/EEA and third countries. To some extent there had been reluctance from third countries on passenger data to be collected from their citizens. Other reasons (where specified by the authority) related to issues regarding the reluctance of third country national carriers to submit passenger data (through a system other than which was already in place). These perceptions are summarised in Figure 7.12 below[252].

Figure 7.12 Types of impacts on third countries as a result of the API Directive



Source: Competent authority responses to the following question in an online survey: To what extent have you observed the following impacts on Third countries?

The carriers commenting on the same question in the online survey also considered that there had been some impact on third countries:

- Two of three carriers considered that API data was requested from third country carriers to a very large extent
- Two of three carries indicated that to some / large extent there had been changes to practices in third country airports
- Two of four carriers indicated that there had been negative influence on relations between EU/ EEA States and third countries. However, two of three carriers also considered that there was no reluctance from third countries passenger data to be collected from their citizens

In addition, some competent authorities considered that the use of API has also strengthened international cooperation on security matters. The adoption of the API Directive has sent a signal regarding commitment towards enhanced security on an international level.

[252] This is based on respondents from 7 to 8 Member States that are currently implementing API and responded to the relevant question in the online survey.

7.4.5 Unintended impacts

The unintended impacts are largely dependent on the Member State concerned, and the way in which they use API data. Unintended impacts tend to be specific to national circumstances and the context in which API systems were implemented.

1) The lack of coherence in the national authorities' requirements for implementing API data negatively impacts carriers

While Member States may have transposed the API Directive into their national legislations, some countries did not have the technical capacity or sufficient resources to process API data. This led to a situation where air carriers sent API data (and bearing the cost of doing so) to national authorities which were wholly or partially unable to use the information transmitted. In other words there were situations where legal obligations with regard to API data existed which cannot be practically carried out.

Similarly, additional requirements of Member States and their deviation from internationally recognised standards in the field meant that carriers had to bear unnecessary additional cost of compliance or had to spend time collaborating with Member State to negotiate a suitable solution. Lastly, the deadline given to carriers to implement API requirements was often too short as it did not take into account the degree of advancement of air carriers' legacy systems.

2) API data were used in some instances for purposes other than border control, migration management or law enforcement.

In some Member States, API data have also on occasion been used for purposes beyond border control, migration management or law enforcement. For example:

- In the UK, at the time of the swine flu outbreak, British Airways had to keep API data on passengers for longer so that authorities could keep a record of persons travelling at that time. The benefits were to monitor the epidemic and take appropriate action;
- In France, a stakeholder mentioned that in the future API data could cater for multiple uses beyond its current purposes; and
- In 12 of the 19 Member States currently implementing API, data on EU citizens is also being processed which was not the direct intention of the Directive

3) API data were used for situational awareness and profiling

As mentioned before, Member States have improved their risk assessment and assessment of threats at the external border by trending API data series. Statistical analyses enabled Member State authorities identify risk factors (i.e. citizenship of passengers, country of origin, flight routes, etc.) which when combined could present a risk to the integrity of the external border or a security risk[253].

4) Synergies in developing and implementing API systems

Although the Directive did not contain incentives for Member States to jointly develop technological solution or systems, some Member States took the opportunity to build on already established systems. For instance, Switzerland adopted many parts of the German API system. To make this possible, the Swiss authorities worked together with the German authorities. This has also raised the level of bilateral cooperation in the field.

Third parties like SITA may also have been able to play such a role in educating their clients as to what solutions they could implement given particular circumstances. However, the cost-synergies derived from private sector companies may have been limited in comparison.

7.4.6 Impact on passengers and airport authorities

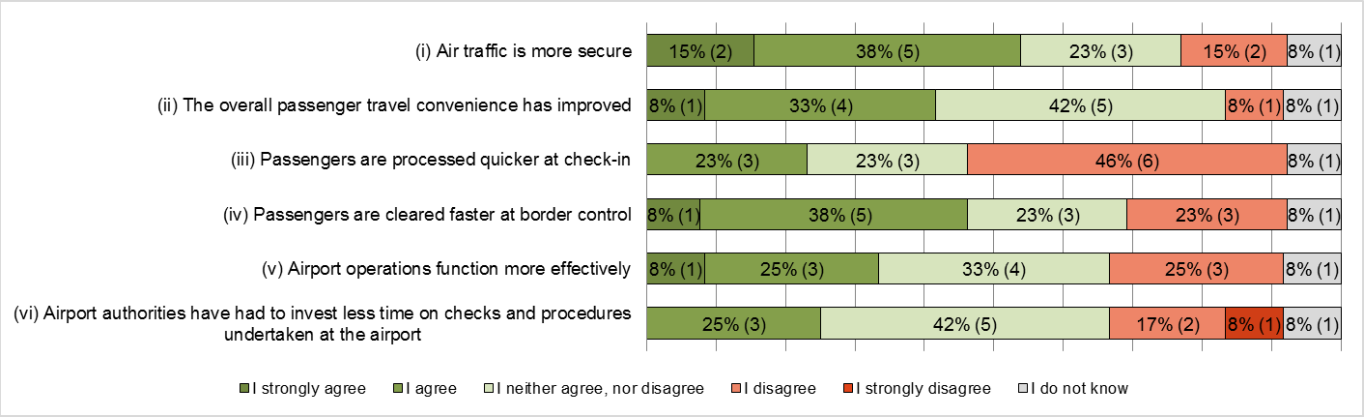
Impacts on passengers and airport authorities seem not to be particularly strong, and there is considerable variation in the views of competent authorities and carriers with respect to

[253] This has at least been the case it Austria, Germany, Italy and Romania

this. Overall, this is difficult to assess with certainty, especially as evidence gathered in this study is based on the perceptions of competent authorities in the Member States and air carriers, rather than the direct opinions of passenger and airport authorities themselves. It has not been possible to organise a full consultation on this aspect.

The competent authorities in countries implementing API systems were of the view that as a result of implementing API the air traffic is more secure and passengers were cleared faster at the border. This view however was not shared by the six carriers responding to the same questions. Only one of the six carriers agreed that airport security had improved and that passengers were cleared faster at the border. Almost half of competent authorities were of the view that passengers were not processed quicker at check-in, which was the view shared by five of the six air carriers. Some competent authorities were also of the opinion that airport operations function more effectively, whereas the carriers mostly disagreed or did not have a view on the issue. Just over a third of competent authorities considered that the overall passenger convenience had improved, whereas again this was not supported by the views from air carriers. Figure 7.13 provides a summary overview of the competent authority perceptions as regards to the impacts of API on passenger and airport authorities[254].

Figure 7.13 The impacts of API data collection on passengers and airport authorities



Source: Competent authority responses to the following question in an online survey: Please comment on the impact of the collection of API data on the following areas.

Some preliminary considerations can also be made with respect to the impact on airport authorities regarding effects on the airport of departure and the airport of destination.

With regards to the impact on the airport of departure, some industry stakeholders were of the view that API systems can cause artificial delays because of data capture (e.g. manual entry), or processing time during checking and on boarding. For example, in the USA, the processing time required to capture API data during peak hours was found to reduce passenger throughput by 17% on average[255]. Another stakeholder calculated that additional processing time amounted to 1 minute 2 seconds per passenger. This was considered to impact negatively on the checking capacity of airports during peak hours either by generating congestion or by obliging airports to introduce additional checking desks. However, this impact may be partially offset by online checking and submission of API data by the passenger in advance of flying for automatic checking purposes.

With regards to the impact on the airport of destination, the competent authorities have pointed out that API systems allow them to better manage border control checks indirectly reducing queuing time of international passengers. In addition, targeted border checks enabled by API systems have meant that any border police intervention or arrest can take place in a more organised way and cause less disruption. The impact on airport authorities

[254] This is based on respondents from 13 to 12Member States that are currently implementing API and responded to the relevant question in the online survey

[255] The stakeholder also considered that “the more manual processing the greater the deviation from standard and the greater the negative impact”.

have been considered positive in the sense that it would reflect positively on the image of the airport and consequently on the Member State.

Another consideration with regard to the impact on the airport of destination has been whether API requirements provide a deterrent for small airlines to fly routes into specific airports subjected to API obligations. In places where carriers only operate infrequent non-scheduled flights, there is no real impetus for carriers to invest in API systems when flying these routes. The carriers might take a conscious commercial decision to fly onto a nearby airport not subject to API obligations or not to fly at all to this destination if cost of doing so undermines the profitability of the route. However, this type of impact has not been observed in this study.

7.5 Added value of the Directive

The following section provides an assessment of the added value of the Directive, or the extent to which EU action has brought added value in comparison to similar Member State level actions and initiatives.

The following has been assessed:

- the overall added value of the Directive; and
- the extent to which unintended benefits and drawbacks of the implementation of the Directive (i.e. spill over effects, etc.) have occurred.

Added value has been assessed from the point of view of the main stakeholders involved in the implementation and functioning of the API Directive.

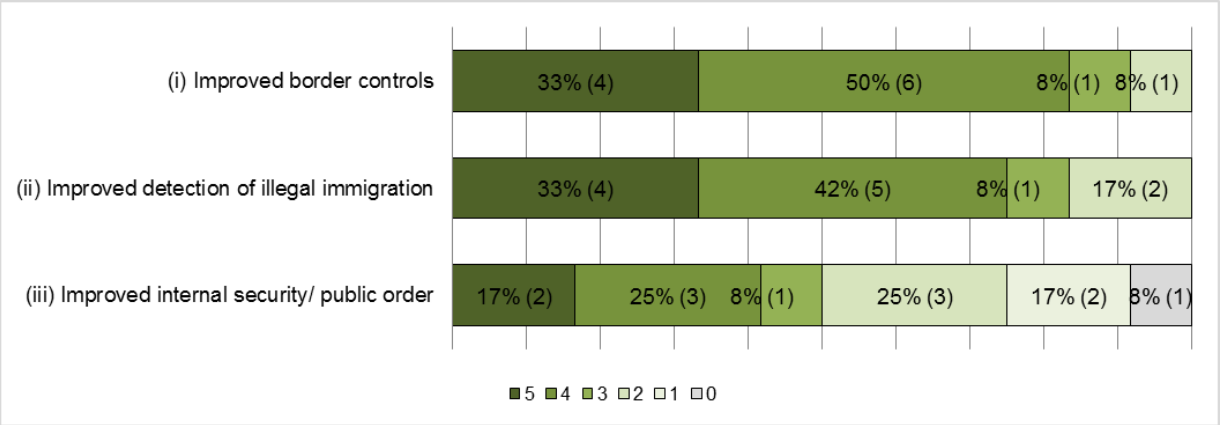
7.5.1 Added value of the Directive for national authorities and air carriers

While some Member States and most air carriers questioned the added value of the Directive, the majority of the national competent authorities considered that the Directive had a specific identifiable added value. Overall the implemented API systems were considered to have a high added value with respect to the achievement of the Directive's objectives regarding improved border control and fighting illegal immigration. The implementation of the Directive also accelerated the timeliness of the adoption of API systems technology and related practices. At the time of the adoption of the Directive a few Member States had planned to implement API systems. About half of competent authorities considered that the Directive had a high or a very high impact on establishment of API systems in the first place. The Directive has also had a very high or high impact on the adoption of new border control practices in about a half of the Member States. The main concerns regarding the added value of the Directive related to the fact that the patchwork implementation reduced its value and that there was no strong business case to support API in some Member States.

7.5.1.1 Added value with respect to implementation outcomes and adoption of new systems and practices

Overall the implemented API systems were considered to have a high added value with respect to the improved border control and fighting illegal immigration. The added value regarding improved internal security was less prominent. Of the 12 competent authorities currently implementing API, responding to the relevant question, ten competent authorities considered that API systems have had very high or high added value on improving border controls and nine considered that there had been a very high or high added value with respect to improved detection of illegal immigration. Only five of the 12 competent authorities considered that the same was applicable to improved internal security / public order.

Figure 7.14 Added value of the API systems with respect to implementation of the API system



Source: Competent authority responses to the following question in an online survey: How would you rate the overall added value of the implementation of the API system with respect to:(i)Improved border controls (ii) Improved detection of illegal immigration (iii)Improved internal security/public order (5 = very large positive impact; 0 = no impact; -5 = very large negative impact)

In addition, the implementation of the Directive accelerated the timeliness of the adoption of API systems technology and related practices. At the time of the adoption of the Directive a few Member States had planned to implement API systems[256]. Although it is not possible to assess with certainty whether or not Member States would never have adopted such systems if the EU Directive was not adopted, its introduction certainly created added value in speeding up the adoption of related technology and new border control management and law enforcement practices.

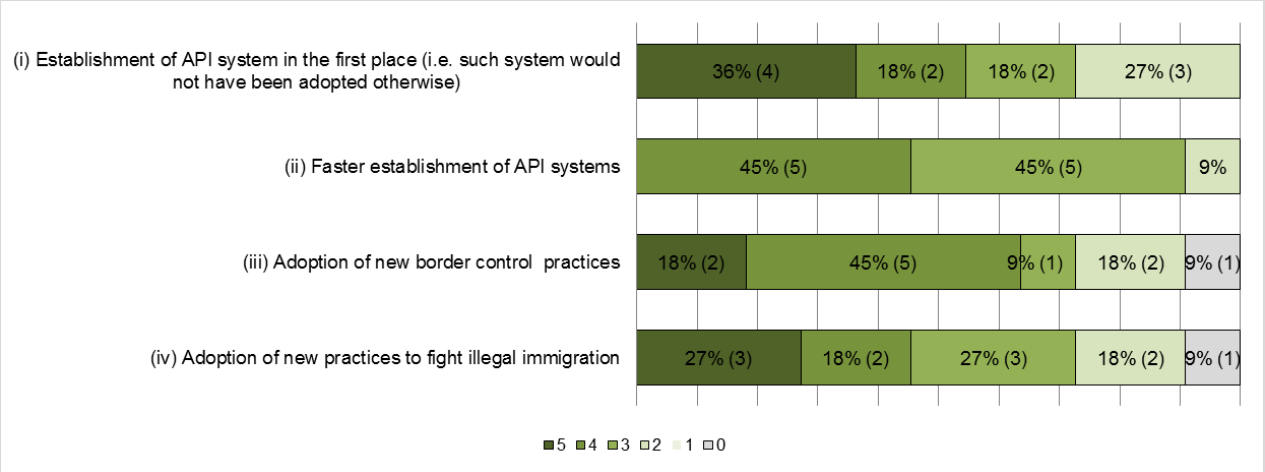
Such practices relate to:

- Efficiency of border control resource planning through better use of technology and existing systems;
- Efficiency of border control checks through creating a new system through which air passengers can be checked in advance, leading to improved border control and enhanced awareness of the operative situation;
- Increased effectiveness in detecting irregular migrants and other wanted persons;
- New practices based on risk-based profiling using API data;
- Improved situational awareness from flights flying from at risk countries and the origin of threats at the external borders; and,
- Quicker reaction and processing of passenger data whereby passengers who are subject to 'alerts' can be targeted in advance to prepare for action. In addition, the level of scrutiny has been enhanced with the prior automated and later manual checks.

The added value of the Directive on the establishment of new practices was relatively high, which is illustrated in Figure 7.15 below. Seven of 11 competent authorities currently implementing API were of the view that the Directive had a very high or high impact on the adoption of new border control practices and about half (n=6) considered that the Directive had a high a very high impact on establishment of API systems in the first place. The competent authorities had mixed perceptions on the extent to which the Directive had led to the adoption of new practices to fight illegal immigration: competent authorities in some Member States considered that the Directive had a very high impact whereas in other Member States they considered that the Directive had low impact or no impact at all in adoption of new practices to fight illegal immigration. In many Member States the Directive had also contributed to faster implementation of the API systems.

[256] i.e. DK, ES, UK

Figure 7.15 the added value of the Directive with respect to the adoption of systems and practices



Source: Competent authority responses to the following question in an online survey: Please rate the added value of the API Directive with in your country respect to the following areas. (5 = very large positive impact; 0 = no impact; -5 = very large negative impact)

7.5.1.2 *Main concerns regarding the added value of the Directive*

The main concerns regarding the added value of the Directive related to the fact that the patchwork implementation reduced its value and that there was no strong business case to support API in some Member States. For example, one of the competent authorities mentioned that air borders are already well regulated, and that the use of preliminary API checks does not remove the need to carry out passport controls at the airports. If the API Directive would help make savings in other operational areas, then it would have an added benefit for controlling air borders. In addition, some stakeholders questioned the depth of the added value for competent authorities as the main impact was only to provide additional time to process data, which would be undertaken regardless at the border. The collection and transmission of API was perceived, from the carriers' perspective, not to provide any added value as there was no commercial need or use for such information, and it did not allow stop suspect persons from boarding the plane in the first instance. Hence it did not specifically improving carrier security.

A sample of six carriers responding to the industry online survey rated the overall added value of Directive as follows:

- **Improved airport security, improved carrier security and improved collaboration arrangements regarding EU/ EEA wide security**: Four of the six air carrier representatives considered that the Directive had no impact on improved airport security, improved carrier security or had improved collaboration arrangements regarding EU/EEA wide security, whereas one carrier considered there was a very low added value in all these respects. One carrier representative considered that API had a high added value with respect to improved airport security and carrier security and a very high added value with respect to improved collaboration arrangements regarding EU/EEA wide security.
- **Upgrade of technology for purposes of API data collection and transmission** and **upgrade of technology for purposes beyond API data collection and transmission**: Four of the six air carrier representatives considered that the Directive had no impact on the upgrade of technology for purposes of API data collection and transmission, whereas three carrier representatives considered that there was no impact with respect to upgrade of technology beyond the purposes of the API data collection and transmission, indicating that Directive was slightly more beneficial for technology upgrade beyond the Directive than the Directive itself. One carrier representative considered there was a very low added value in upgrade of technology for API purposes and two considered that there was a low added value purposes beyond API data collection. One carrier representative considered that API had a very high added value with respect to both

upgrade of technology for API data collection and transmission proposes and beyond the specific requirements relating to API.

- **Improved effectiveness of balancing security with airline business operations**: Three of the six air carrier representatives considered that the Directive had no impact on improved effectiveness of balancing security with airline business operations, whereas two carrier representatives considered there was a very low added value with respect to improved effectiveness of balancing security with airline business operations. One carrier representative considered that API had a very high added value in this respect.

7.5.2 Unintended benefits and drawbacks to the implementation of the Directive

From the airline industry's perspective the API Directive did not bring benefits for air carriers. One of the concerns mentioned was that the Directive did not specify standards and implementation guidelines which would have enabled more joined up implementation at EU / EEA level. According to industry stakeholders, this resulted in a patchwork implementation in each Member State where requirements and obligations imposed on air carriers deviated from internationally established best practices. The end result is that the various national requirements have had a negative impact on air carriers flying routes to Europe.

In addition to the above, the airline industry had additional reservations regarding the Directive and its intended benefits:

- One stakeholder considered that some small airline companies (e.g. small African airlines) may have been prevented from flying routes to the EU when considering the cost – benefit ratio of doing so, arising from the API obligations;
- Another industry stakeholder pointed out that in particular circumstances the business case for the adoption of API system might not justify the costs, given expected benefits, particularly when there was no clear implication that API would help deter irregular migration in large numbers;
- Some industry and national competent authorities argued that the API systems falls short of national authorities' ambitions because irregular migrants willing to enter illegally into Europe do not favour air transport to enter illegally in Member States and use other modes of transport. Similarly, the API system would not effectively allow for the identification of terrorist as they often do not travel with their real identification documents;
- Some industry stakeholders also argued that the way the Directive was implemented was a missed opportunity to enhance aviation security and avoid return costs since the Directive stayed away from interactive API systems where a suspect person could be refused to board the plane in the first instance.

On the positive side, there are some marked unintended benefits that can be seen to have materialised as a result of the adoption of the API systems:

- **Investment in systems and infrastructure**: For example, some countries (such as Switzerland and Italy) have invested in national systems to deal with API flows in a technologically advanced manner. There may also be indirect benefits to other system infrastructures. For example, from the carriers' perspective, the Directive was considered to be slightly more beneficial for upgrade of technology for purposes beyond API data collection and transmission than the Directive itself. This indicates that wider system-wide benefits have been / and are likely to be realised in the future.
- **Border control practices**: one of the most prominent unintended benefits has been the impact on the adoption of new border control practices. Data is processed and second-line checks carried out more effectively, enabling appropriate measures to be planned in good time. Going further, in some Member States the API data has enabled undertaking risk analysis to better understand and target specific migration routes.

In addition, although not directly stated, there is a high probability that the widespread adoption of API systems may have created a level playing field for such systems, increasing

innovation and sharing of good practice in the future, given that many have only recently adopted such systems. Similarly, the widespread adoption of related technologies may help drive down the cost of such systems as the industry implemented these systems on an "industrial scale" rather than in a discrete and much tailored way.

8 Conclusions and recommendations

This section provides main conclusions and recommendations regarding the study.

8.1 Main findings and conclusions

This section summarises the main findings and conclusions of the study and is structured as follows:

- 8.1.1 – Main findings and conclusions regarding the transposition of the Directive and its coherence to other legal instruments;
- 8.1.2 – Main findings and conclusion regarding the functioning of the Directive /API system procedures;
- 8.1.3 – Main findings and conclusions regarding the relevance and outcomes of API systems;
- 8.1.4 – Main findings and conclusions regarding the cost efficiency of the API systems; and
- 8.1.5 – Main findings and conclusions regarding the added value of the Directive

8.1.1 Main findings and conclusions regarding the transposition of the Directive and its coherence to other legal instruments

The majority of Member States were judged to have gaps in the transposition of the Directive and to have incompletely or incorrectly transposed one or more of the Articles laid down by the Directive. Only Slovenia was judged to be in full conformity of the Directive[257]. The main issues regarding the transposition related to data protection and data transmission concerning the transposition of Article 6; this article embraces the provisions governing the collection and processing of API data and as such, it is one of the core articles of the Directive. A more detailed analysis of the specific data protection issues is provided in subsection 8.1.1.1 below

The overall assessment of the quality of the transposition has shown that:

- The majority of the Member States transposed the Directive later than the deadline laid down by Article 7 of the Directive (5th of September 2006). In some Member States, like Spain and the UK, transposition was only partially late whereas some other Member States (like Bulgaria, Romania and Switzerland) only transposed the Directive when accessing the Schengen *acquis;*
- Seven Member States have incorrectly or not transposed the provision set in Article 4 of transposing either a minimum or a maximum amount of the sanctions to be imposed to carriers who do not comply with the requirements laid down by the Directive.
- Nine Member States allow the authorities to store the data for longer than 24 hours after transmission without respecting the criteria set by the Directive. The incorrect transposition of this provision (Article 6.1, third paragraph) has been deemed as a major non-compliance issue since the time limits are establish in order to ensure that API data are handled in a manner that does not affect the fundamental data protection rights of the passengers concerned.

Seven Member States[258] do not comply with the obligation for carriers to delete the data within 24 hours of the arrival of the means of transportation. Directive also allows Member States to adopt two additional measures, namely the imposition of additional sanctions to carriers for serious infringements of their obligations and the use of API data for law enforcement purposes. Less than half of the Member States have opted for imposing

[257] For more information on the methodology used for the conformity checking analysis of the national legislation with the API Directive, please see Section 2.4.1.

[258] AT, DK, FR, IS, NO, PL and the UK

additional sanctions. The issue of law enforcement has raised some concerns and has been summarised in section 8.1.1.2 below. In addition, the Directive also offers the possibility for Member States to extend the scope of the national transposing measures also to non-air carriers. The reasons for this extension in the Member States that opted for it vary and have different impacts in the national legal orders as discussed in section 5.2.7.

Sections 8.1.1.1 to 8.1.1.3 further elaborate the wider implications of key issues that have emerged from the transposition of the Directive.

8.1.1.1 *Issues regarding safeguards for data protection*

The transposition of the Directive has shown that in certain Member States the safeguards regarding data protection included in the API Directive are not explicitly transposed by the national legislation. The main concerns arise regarding the following matters:

- Authorities are allowed to keep the data for more than 24 hours if those data are to be used for 'statutory purposes', but nine Member States allow the authorities to keep the data for more than 24 hours for purposes that go beyond their 'statutory purposes'. Some countries such as France and the UK allow for a storage time of up to 5 years, which may conflict with data protection legislation at EU level.,
- Seven Member States have been identified as not complying with the obligation for carriers to delete the data within 24 hours of arrival of the means of transportation. This may also be contrary to data protection provisions. Moreover, the following conformity issues emerged from the legal analysis of the transposition of the Directive:
- All Member States have transposed the obligation for the carriers to transmit the data to the competent authorities contained in Article 3 and which constitute the core of the Directive. The list of which data need to be transmitted has not been interpreted as being exhaustive and hence some Member States have gone beyond and require more data. It is for the Commission to assess whether the legal basis used for this additional collection would imply a breach of data protection law. In addition, although the cross-reference that transmission shall be done in accordance to Article 26 of the Schengen Convention as supplemented by Directive 2001/51 is only present in the legislation of seven Member States, this has been considered as a minor issue of compliance since the Schengen Convention and Directive 2001/51 are in any case transposed into the national legal order of every Member State.
- Most of the Member States that have not transposed the requirement of saving the data in a temporary file in their national legislation have nevertheless incorporated the obligation for carriers and authorities to delete the data in 24 hours (see below) which means that no problems would arise in practice. However, three Member States (Austria, Iceland and the Czech Republic) have not transposed any of the requirements and, hence may be in breach of data protection legislation.
- The majority of Member States have transposed the obligation for carriers to inform the passengers of the collection of their data, although ten of them have not made a cross-reference to the Data Protection Directive as required by the API Directive. This shall be considered as a minor issue, since the Data Protection Directive has been transposed in all Member States. However, attention shall be paid to those Member States which have not transposed the obligation to inform passengers: Austria, Denmark, Finland, Iceland and Norway.

8.1.1.2 *Collecting and processing API data for law enforcement purposes*

Although Article 6.1. *fine* offers the possibility for Member States to use API data also for law enforcement purposes, the Directive does not provide a binding definition of what constitutes law enforcement purposes. An indication of what national authorities may interpret as law enforcement is contained in Recital 12, i.e.: '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'. Member States have enacted legislation allowing for the use of API data for purposes ranging from the fight against terrorism to providing intelligence to combatting crime giving many different interpretations to this clause.

The purpose for which data are used is a key element when determining whether or not the processing of those data is in line with European data protection legislation and hence, the determination of what falls within the definition of law enforcement is fundamental in framing the purpose limitation as required for by the Data Protection Directive. The Commission may consider the possibility of clarifying the definition of law enforcement purposes in this context in order to guarantee that the API data are used in a manner compatible with the principles informing data protection legislation.

8.1.1.3 Data processing for third country nationals and EU citizens

The Directive did not make a distinction between EU citizens and third country nationals in carriers' obligation to collect API data. In practice, most countries collect API data from all passengers from a particular flight/journey, whether they are third country nationals or EU citizens. Only five Member States[259] specifically differentiated in their transposing legislation between third country nationals and EU citizens regarding the collection of API data. With respect of data processing, evidence gathered as part of this study indicates that at least 12 of the 19 implementing countries process information on EU passengers when checking API data.

The main intended purpose of the Directive has been to collect data from passengers arriving from third countries for improved border control/immigration purposes. Processing data on EU citizens may bring a risk that in the longer-term checks might become systematic which might go against to the free movement of persons *acquis.* Some carriers have already refused to transmit data to the United Kingdom on certain routes as it collects API data of EU citizens, on intra-EU flights, while the Directive only applies to flights from third countries.

8.1.2 Main findings and conclusion regarding the functioning of the Directive /API system procedures

This study has shown that in the nineteen Member States that currently implement API systems, the systems' technical and operational capabilities are varied, and the operational procedures that underline the API systems are inconsistent. This has created some incoherence and uncertainty in the way in which API systems are operated across the EU and EEA.

The main API system issues relating to the procedures can be summarised as follows:

- In all Member States API data is captured by carriers, either through automated means (e.g. reading MRZ passport data), online booking system[260] or through entering data manually at check in. Manual data entry in particular is susceptible to errors, but no immediate solution can be found as financial investments by carriers and airport authorities are required to invest in software systems and hardware, which in some occasions may not be cost effective[261]and generally require longer-term investment.
- API data may be transmitted at check-in (e.g. Austria, Czech Republic, Cyprus and Hungary), on boarding (e.g. Italy, Romania, Germany, Netherlands, Spain), or at departure (e.g. Estonia, Ireland, Malta and Switzerland). In some Member States the time at which API data is transmitted is dependent on the route. The time window allowed for data processing may be crucial to allow for proper checking, though standardisation in this respect may not make sense. Additional considerations such as the route and necessary checks on validity and completeness of the data prior to transmission are be more important for ensuring the correct and effective use of data by competent authorities
- Member States use different mechanisms to receive the API data, some may use a third party service to transmit and receive API data (e.g. SITA or ARINC) which will also parse the API data from the format used by the carriers into the format required by the

[259] Five Member States (BE, HU, NL, LT, LU) specify that API is to be collected only on third country nationals. No information is available for other Member States – see section 5.1.2.

[260] On occasion, depending on the carrier, API data is also captured through an online system at booking, although the final check is to be carried out at check in to ensure the correct identity of the person.

[261] In particular in instances where a carrier operates a limited service on a certain route.

border management authority; whereas some countries also use their own specialist software systems[262]. In addition to these types of systems, many countries also use manual methods of transmission, such as email, pdf, fax, which pose a risk to data security and may create processing inefficiencies. In practice, Member States use more than one mechanism for data transmission[263]. The manual data transmission mechanisms are not optimal, and in addition to security risks, they make it more difficult to run checks on databases, particularly when the data transferred is in a non-electronic format.

- Member States process data through automated means or check data manually. In practice data is always checked manually following automated checks. Several competent authorities indicated that they faced issues with data quality, when matching API data with those of other databases, including SIS I and SIS II, VIS, EURODAC and national police watch list due to incomplete or incorrect data entry[264]. Overall, issues with API data processing are due to data collection mechanisms that do not support automated capture of data from the passport directly but which instead require manual entry, leading to higher probability of errors occurring, and transmission means which are manual and in some instances may pose risk to data security.

The main contextual matters which have influenced the focus of API system procedures and which have created additional costs to carriers include:

- API data content requirements are in some Member States different to those required in Article 3 of the Directive[265] and although most countries collect API in a standard compliant with the UN-EDIFACT, not all do. The fact that data field requirements vary slightly across Member States creates confusion. For carriers having to comply with varying data requirements adds to their administrative burden and carriers may need to in some instances assess the legitimacy of the request and decide whether to agree to transmit the data. In particular adding new data field requirements and flight routes can become a somewhat costly exercise for the airline data collection and transmission systems that have been pre-designed to particular requirements.
- The routes for data collection and transmission are variable; some countries collect API data on all non-EU flights arriving in the Member State whereas others target the collection of API from only those third countries considered at risk of irregular migration or to be 'source countries' of irregular migration. From cost effectiveness point of view it makes sense to target certain routes, though it cannot be concluded this is the best method given that others might consider such practice to be discriminatory. Member States are left with the choice of deciding the magnitude of API data collection.

Accordingly, the API system related procedures have room for improvement regarding the specific data content and format, the extent to which carriers use the most efficient and secure means for data collection and data transmission and the extent to which the processing of API data is optimal given the difficulties with data matching. Improvements in this regard would make procedures more lean and compliant and increase the effectiveness and impact from the use of API data.

[262] For example in ES, CZ, RO, CH, DE and NL.

[263] For example, data in Germany can be transmitted through specialist software, via encrypted email but also via fax. Hungary receives API data in various forms including fax, pdf documents, and paper copies. In addition, Cyprus and Hungary send API data via fax, though they also send data via specialised software (e.g. SITA / ARINC).

[264] Issues with data quality may equally relate to those of the databases, rather than problems with the API data received. The origin of error cannot always be clearly identified.

[265] For example, Spain does not require the expiry date of the travel document unlike other countries, so carriers have to filter this field out of the passport data collected when transmitting API data. Italy requires carriers to provide passengers' place of birth and Germany requires passenger gender and the complete flight route.

8.1.3 Main findings and conclusions regarding the relevance and outcomes of API systems

API systems have been only very recently set up, and half of the systems currently operational are in a pilot phase: Nineteen Member States[266] (62% of 31 countries) currently implement API systems,[267] with nine of these Member States operating a pilot system. Main reasons limiting the effectiveness of API systems are due to gradual implementation since their establishment. Most API systems were tried and experimented in the first years of their implementation and on a reduced scope (i.e. on a sample of third countries, on a sample of Border Crossing Points, or only on some vessels)[268]. Given the current early implementation cycle, the full impacts and overall cost efficiency of the API systems can be only concluded to some extent. Further evidence (in terms of outcomes data) needs to be collected and API systems' impact monitored by the authorities. In spite of this, several conclusions can be made with respect to API systems' match to the needs of member States and the overall exemplary impacts of the API systems.

8.1.3.1 The relevance of Directive's objectives to the needs at national level

The study has indicated that the perceived national needs at the time of transposition largely aligned with the objectives of the Directive to combat irregular migration and to improve border controls. Most Member State competent authorities considered that the objectives of their API system or legislation were fully in line with those of the Directive. However, some Member States pointed out that in practice because of implementation issues the intended objectives could not be fully pursued.

Member State competent authorities also identified law enforcement as a perceived need at the time of transposing the Directive. For example, the stakeholders consulted reported that combating organised crime, apprehending known criminals, fighting the import / export of illegal drugs and informing intelligence services of potentially dangerous persons and fight against terrorism were amongst the main policy needs at the time of transposing the API Directive. At least three Member State stakeholders perceived the Directive as relevant to national needs mainly to the extent that Directive 2004/82/EC allows for the use of API for the purpose of law enforcement.

The lack of binding definition of 'law enforcement purposes' for which API data can be used[269] has led Member States to use API data according to law enforcement activities most relevant to them. The overall scope for 'law enforcement' has taken many meanings from public security, to terrorism to combating serious crime and to other less severe criminality, including petty offences. The API Directive is therefore currently being used to aid several law enforcement efforts, some of which may not be desirable within the intended main objectives of the Directive. This has blurred the focus of the potential data processing purposes and use of the API data.

8.1.3.2 The effectiveness and impact achieved by implementing API systems with respect to the main purposes of the Directive

The use of API data has made border checks faster, and enabled faster reaction against suspect illegal migrants and suspect criminals. To an extent the Directive has also increased technological innovation in those Member States that have adopted technologically advanced API systems. As a consequence of the API systems, the border management authorities have become better prepared for their general border control activities.

The implementation of API systems has helped to improve border controls, as data has been received in advance, providing additional preparatory time and an ability to target in advance

[266] AT, CH, CY, CZ, DE, DK, EE, HU, IE, IT, IS, LV, LT, LU, MT, NL, RO, ES, UK

[267] This includes Liechtenstein, which is covered by the Directive, but which – as highlighted in Section 5 has no airport and so cannot introduce the provisions of the Directive as they mandatorily apply to air travel.

[268] DK, FR, RO, UK

[269] The Directive does not provide a binding definition of what constitutes 'law enforcement purposes'. An indication of what national authorities may interpret as law enforcement is contained in Recital 12, i.e.: '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'.

passengers who are subject to an 'alert'. The level of scrutiny of this task has been reinforced with the prior automated checks and subsequent detailed checks that are being carried out. For instance, through API systems, competent authorities have been able to:

- Identify specific flights for which enhanced border checks are necessary (i.e. as compared to other flights) because the higher prevalence of non-EU nationals in those flights is known before landing[270];
- Better prepare for the control of specific passengers by identifying them via API data in advance of their arrival. It helps to accelerate border checks because suspected illegal immigrants can be separated from the other passengers and reallocated to separate lanes without the other 'rightful' passengers queuing and waiting[271];
- Anticipate certain situations and anticipate and classify the type of controls to be performed[272];
- Check API data against other databases, and thus shorten the time for controls and checks at the external borders[273].

With respect to immigration control, API has had the most distinct impact in relation to improved management of staff used to combat illegal immigration and improved targeting of suspect illegal immigrants. API also had an impact on improved knowledge of migration routes and to an extent had increased refusal of entry to illegal immigrants. Risk profiling has played a big role in this respect whereby authorities have studied the routes for illegal immigration and the profile of activities that person had done to conceal the identity (e.g. destroying travel and identification documents). There is evidence to suggest that API systems have contributed to reducing irregular migration in the following ways:

- By improving risk-based profiling of international passengers[274]. For instance, authorities can now detect illegal practices through risk profiling in a way it was not possible before[275].
- Increasing the rate of detection of persons trying to enter the territory with lost or forged documents[276] especially when they are designated as 'forgers' in the SIS[277]; and
- For 'blocking' access of irregular migrants attempting to transit external borders via airport hubs– by identifying the main countries of origin of such persons and controlling passenger lists[278] or through the identification of groups of migrants on the basis of the information relating to flight reservations made for several persons

At least twelve Member States have used API data for law enforcement purposes with the most marked impacts relating to an enhanced internal security and public order. Use of API data has had very little or no impact with respect to collaboration with other countries regarding law enforcement efforts but had some impact in increase in the arrest of criminals in few Member States. The specific roles that API data have played include preventing crime and terrorism and identifying persons who have been identified as a security risk by law enforcement authorities. Competent authorities in four implementing countries also pointed

[270] AT

[271] DE, LU, RO

[272] FR

[273] AT, CH

[274] DE, EE, RO

[275] These practices consist in buying a flight ticket to another destination country with a transfer of flight in one EU Member State (e.g. Germany). At the time of transit, some irregular migrant throw away their travel documents and disembark in this Member States (e.g. Germany). Before the Directive came into force it was hard or often impossible to find out the names of these persons and where they came from. Having observed this phenomenon for years the police figured out on which routes this practice is the most prevalent and can "profile" the passengers who are most likely to do this.

[276] DE, LV

[277] LV only

[278] FR

out that the use of API data has helped to investigate criminals, arrest criminals and convict criminals[279].

In addition, although impacts from use of API data can be evidenced, their magnitude in a consistent way cannot. This is because authorities (with the exception of few Member States) do not collect specific data that would allow for direct measurement and monitoring of the effectiveness and impact of the API systems.

8.1.3.3 *Impacts on other stakeholders beyond border control, immigration and law enforcement activities*

The study has shown that the impact of the Directive on third countries and on international relations has been relatively limited. There have been little impacts on third countries apart from that API data have been requested from third country carriers and changes in practices of third country airport operators have taken place. No major complaints have been noted by third countries regarding the data collection. Moreover, impacts on passengers and airport authorities were not particularly strong, and there was considerable variation in the views of competent authorities and carriers with respect to this: although the competent authorities in Member States implementing API systems were of the view that as a result of API the air traffic is more secure and passengers were cleared faster at the border this was not shared by the carriers. In general, carriers have a rather negative perception of the impact from the implementation of the API Directive as they considered that it had imposed an administrative and financial burden for the airlines from which they did not see benefits to their own objectives and operations, including that of passenger facilitation and carrier security.

8.1.4 Main findings and conclusions regarding the cost efficiency of the API systems

Overall assessment of cost efficiency has been challenged by the lack of systematic data although clear conclusions can be made regarding the cost implications of API systems. From the competent authorities' perspective, API systems have had an impact at a reasonable cost. None of the authorities thought that API was not cost efficient at all, but the perceptions of overall efficiency ranged from very low to very high, with most respondents indicating medium-level cost efficiency.

There is considerable variation across the Member States with respect to the costs incurred:

- The costs for Member States implementing API varied from €9k per annum (pilot in one airport) to €4 million per annum for a highly advanced technological system, which includes ability to access airline system to collect the data and undertake sophisticated analysis for risk profiling and intelligence purposes.
- For an all-encompassing system (such as e-Borders in the UK), in which the API data stream forms a small part, the costs of implementation were estimated at €175 million by the competent authority, with the cost of first year of operation approximately at €20 million.
- Overall, the API Directive-related compliance costs for carriers ranged from less than €0.5 million to over €2 million on average per carrier per annum after the set-up costs had been absorbed

The main conclusions regarding the overall efficiency relate to the following measureable factors, available in few Member States:

- Over the past two years (2010-2011) in Austria, action has been taken against 0.4% of all international passengers whose API data had been collected;
- In the past year (2011) in Italy, action has been taken against 0.7% of all international passengers whose API data had been collected;
- Over the past four years (2008-2011) in Germany, in approximately 7% of flights for which API data had been collected a wanted person was recognised by the system, which means that on average 1 in 14 flights a match is made to a wanted person / person subject to an alert

[279] This has been relevant for at least the following Member States: AT, IT, RO and UK.

Although the extent to which the costs are justified against the above measurable actions (also taking into account the very recent implementation of the API systems) cannot be fully concluded, it is certain that the use of API data has yielded benefits against the costs incurred for the competent authorities in the Member States. From the carriers' perspective this has not been the case as they are yet to realise benefits from their financial investments related to the implementation of their obligations.

8.1.5 Main findings and conclusions regarding the added value of the Directive

The Directive has brought added value to the national competent authorities in charge of border control and law enforcement through several means, primarily through accelerating the adoption of API systems, increasing the capacity to process information faster in order to identify illegal immigrants and suspect criminals and through establishing more innovative border control practices. At the time of the adoption of the Directive only few Member States had planned to implement API systems[280].

Although it is not possible to assess with certainty whether or not Member States would never have adopted such systems if the EU Directive was not adopted, its introduction certainly created added value in speeding up the adoption of related technology and new border control management and law enforcement practices:

- API systems increased the efficiency of border control resource planning through better use of technology and existing systems;
- The use of API data facilitated the adoption of more advanced border control checks through creating a new system through which air passengers can be checked in advance, leading to improved border control and enhanced awareness of the operative situation; and
- The processing of API data increased effectiveness in detecting irregular migrants and other wanted persons

The main concerns regarding the added value of the implementation of the Directive related to the patchwork implementation of API systems across the EU. In some Member States there was not a strong business case to support such systems, particularly when air borders were already strongly regulated and the routes through which irregular migration takes place did not include air travel. In addition, competent authorities concluded that the use of preliminary API checks did not remove the need to carry out passport controls at the airports or help make savings in other operational areas. From carriers' perspective API systems did not provide any added value as there was no commercial need or use for such information, and it did not allow stop suspect persons from boarding the plane in the first instance in order to improve carrier security.

The added value of the Directive cannot be fully realised when some Member States have not implemented API systems. Of the eleven member States which have not (yet) implemented API systems at least six (Belgium, Finland, Lithuania, Norway and Sweden) specifically cited technical difficulties as the reason for not implementing them. For example, in Lithuania and Norway passenger data is not currently transmitted electronically, hence the API systems cannot be fully implemented. Belgium, Finland and Greece also reported technical problems of interoperability with the airline data transmission system and the systems operated by the border control authorities. In Finland, for example, the focus has been to implement API system that is technologically advanced, but which does not substantially increase costs for the national carrier, and also does not require manual data transmission. There are synergies to be gained from EU-wide implementation and Member States should be prepared to share technical information on how to best implement API systems. Such exchange would also be useful in countries that already implement API systems but where improvements could be made.

[280] i.e. DK, ES, UK

8.2 Main issues and recommendations

To complement the main findings and conclusions presented in Section 8.1, this section details the potential contentious issues unveiled by the study and provides recommendations with respect to key themes related to the Directive. The recommendations have been grouped under three headings:

- Quality of transposition and interpretation of the provisions of the Directive by Member States;
- Functioning of the Directive and implementation of API systems in the Member States; and
- Monitoring and evaluation mechanisms and arrangements.

8.2.1 Quality of transposition and interpretation of the provisions of the Directive by Member States

Main issue 1

This study evidenced instances of potentially incorrect or incomplete transposition of the Directive in the Member States implementing measures; most of which are minor or without major apparent impacts on the functioning of the Directive. Potential issues relate to:

- *Use of API data for "law enforcement purposes"*: The study evidenced the various interpretations by Member States of Recital 12 of the Directive on the use of the Directive for law enforcement purposes[281]. However, Recital 12 is not binding and hence, provides only the basis for what seems to be a wide variation of interpretations of the concept of 'law enforcement'. *List of API data requirements:* The list of data provided by Article 3.2. of the Directive has been interpreted by Member States as not being exhaustive, and, hence, Member States have sometimes gone beyond the exact wording of the Article. This may pose a problem if Member States collect data that may not be considered as proportional and adequate for the purposes of the API Directive.
- *Sanctions*: In 2011, seven Member States had not transposed the minimum and maximum amounts of sanctions foreseen in Article 4 of the Directive. Conversely, ten Member States implemented additional sanctions (in line with article 6.1 of the Directive). As a result, sanctions have been applied unevenly across Member States either applied to a great extent as in the case of a few Member States [282] or not at all as in the majority of cases[283].
- *Issues of data protection:* The evaluation indicates that nine Member States allow the authorities to keep the data for more than 24 hours for purposes that go beyond their 'statutory purposes'. In some countries storage time can go up to 5 years, which may conflict with data protection legislation at EU level, and should be assessed by the Commission. Additionally, seven Member States do not comply with the obligation for carriers to delete the data within 24 hours of arrival of the means of transportation.

Recommendation 1.1 – on the use of API data for law enforcement purposes

The Commission would need to clarify the legitimate uses of API data for law enforcement purposes. This might include but might not be limited for example to the enforcement of border security, internal security, custom, national security related legislations[284].

Recommendation 1.2 – on the list of API data requirements requested by the Member States

[281] Legislation in 18 Member States mentions the use of API data for enhancing internal security and public order, including fight against terrorism.

[282] As in the case of Austria and to a lesser extent in Germany and Czech Republic on grounds of incorrect information transmitted by carriers.

[283] i.e. all Member States implementing API systems but AT, CZ, HU, LV, RO and DE.

[284] Note that restricting the definition would have a detrimental effect on existing API systems as a number of Member States primarily use API data for the above mentioned purposes.

The Commission would need to clarify the extent to which Member States can go beyond the list as mentioned in Article 3.2 of the Directive, and examine whether the categories of additional data can be considered as proportionate and adequate for the purposes of API. Providing that the Guidelines on Advance passenger information from the ICAO/IATA/WCO recommend a maximum set of API data to be transmitted by carrier, it is recommended that the Commission follows a similar approach.

Recommendation 1.3 – on the use of sanctions and their nature

The Commission would need to ensure the correct application of the obligations of the Directive. Actions for the Commission would include:

- Contacting Member States and taking appropriate action to ensure they correctly transpose minimum and maximum amounts of sanctions foreseen in Article 4 of the Directive.

Recommendation 1.4 – on data protection rules

The Commission would need to ensure the correct application of the obligations of the Directive. Actions for the Commission would include:

- Contacting Member States and taking appropriate action to ensure they correctly transpose the time limitation for the retention of API data by both the carriers and the authorities. Guidelines and recommendations would be particularly pertinent with respect to data retention period for the purposes of law enforcement, access restrictions to API data by authorised officials, and the minimum safeguards required for data transmission and data retention. One of the expected impacts of these recommendations would be the Data Protection Authorities to inspect API systems to verify their compliance with data protection laws on the basis of a clear guidance issued by the national legislators.

Main issue 2

This study evidenced that in some instances the application of the Directive could lead to issues of coherence with other relevant EU legislation. There are potential issues relating to:

- Legislation on freedom of movement of persons and concerns among some Member States that API data is being collected on intra-EU flights – e.g. in the UK and Spain. This might also mean that obstacles have emerged precluding EU citizens and their family members to fully enjoy their right to move and reside freely

Recommendation 2.1 – on coherence with the freedom of movement of persons

- The study evidenced potential conflicts between the Directive and the principle of Free Movement of Persons with regards to the collection and processing of data of EU citizens. The Directive does not distinguish between third country nationals and EU citizens and no case of explicit breach of a particular instrument has been reported to date. However, the issue has been raised by the European Parliament and some Member States have expressed their concerns on the risk of systematic checks on EU citizens which are forbidden. Hence, it is recommended that the Commission clarifies the scope of application of the Directive with regard to EU nationals and intra-EU flights

8.2.2 Functioning of the Directive and implementation of API systems in the Member States

The main issues and related recommendations regarding implementation are:

Main issue 3

This study evidenced instances of late or patchy implementation of API systems, or in some cases failure to implement API systems. Potential issues related to

- **Lateness in or absence of the implementation of API systems in Member States**:
  - At the end of 2011 six Member States had not implemented API systems and two had no plan to implement them in the near future. Reasons cited for not

implementing API systems were that the costs of implementing API systems were comparatively high to expected benefits and technical difficulties in the implementation

- **Sub-optimal implementation of API systems:** There are important variations in terms of the scope of application of API systems, their features and their functioning. For instance:
  - *Geographical scope of application*: There is variation as to the scope of API data collected in Member States, with some countries collecting API on all non-EU flights arriving in the Member State and others targeting the collection of API from only those third countries considered at risk of irregular migration or to be 'source countries' of irregular migration.
  - *Type of carriers subject to API obligations:* Most implementing countries collect API only from passengers on air carriers, although a few also collect it from sea carriers. The reasons for limiting the scope of data collection to air carriers are not always clear, but seem to be related to a lack of prioritisation due to the fact that, the API Directive provides only that API is collected from air passengers, with the collection from other carriers being optional. Another reason may be a lack of financial resources.
  - *Consistent standards:* The features and characteristics of API systems have not been standardised across the EU / EEA and, subsequently, implementing countries place different requirements on carriers. Divergence in standards have been evidenced for:
    - The format of the data collected is sometimes not compliant with UN-EDIFACT;
    - The timing of data capture and transmission of API data vary across Member States. It is determined in some Member States by security considerations (i.e. API is only transmitted once there is no further opportunity for the passenger to leave the vessel) or by considerations of the duration of the journey (i.e. if the journey is short, API is sent prior to take-off to allow enough time for BMAs to process the data).
    - The extent to which the transmission of API data is automated: Half the implementing Member States receive API data which have been transmitted through non-automatic means such as fax and email. Most implementing countries consider an automatic system the best solution for securing personal data, as they apply higher levels of data protection than those which allow for non-encrypted data to be sent (e.g. via email) or which allow multiple and synchronous access to API data.
  - Quality of API data collected: The effectiveness of data collection and data quality depend on the systems and processes in place to capture, transmit, process and match the API data. This study evidenced issues at each stage of this end to end process but primarily during:
    - Data capture: There may also be infrastructure difficulties in some airports in third-countries, which make it difficult to set up non-manual systems of data capture.
    - Data matching: About half national competent authorities surveyed indicated that they faced issues with data quality, when matching API data with databases including SIS I and SIS II, VIS, EURODAC and national police watch lists.

    In general a lack of harmonisation in standards and sub-optimal implementation had cost implications for carriers in terms of development, set-up costs and operational costs and for competent authorities in terms of data clean up, processing errors, costs of systems, effectiveness and efficiency of systems.

Recommendation 3.1 - on the adoption of API systems for those Member States that have not implemented API systems

The Commission should adopt measures to incentivise Member States to invest in API systems or upgrade their existing API systems. Actions the Commission could undertake include:

- Draw attention to the results from the future Frontex study on a cost-benefit analysis on API systems and best practices from the study to exemplify how best implement API systems
- Encouraging the joint development or technological innovation for API systems, potentially to help reduce the costs of implementation and also to increase the API systems' coherence in the EU/Schengen area and application of common standards. This could also have the benefit to spur innovation if implemented through research grants to consortia mixing industrial and public sector partners.
- Supporting the exchange of good practices between competent authorities to maximise the benefits from the implementation of API systems. The themes best suited to exchanging practices include
  - Benefits of and approaches with regard to risk analysis
  - Benefits of and methods for extending of API systems to other carriers (i.e. maritime and land transport mode)
  - Efficient mechanisms used for API data capture, transmission and reception, data processing capability, data matching and methods for realising the full benefits of API systems
  - Efficient integration of API systems with existing database and with physical checks at the border, in order – for example – to identify migrants who destroy documents mid-flight and/or 'switch' identities (e.g. by including biometrics).
- Supporting exchange of personnel between competent authorities and capacity building activities such as training, technical assistance, etc. This will help building a community of practice with regard to API systems in the EU.

Recommendation 3.2 - on standard mechanism for the automated data collection, transmission of API data from carriers

- The use of standard mechanisms for the automated data collection would help to address issues regarding data capture (ineffective mechanisms of capturing API data, inconsistent data field requirements), data transmission (mechanisms used for transmission and receipt are not inter-operable) and data processing (difficulties in data matching and systems processing). Actions for the Commission could include:
  - Adopting guidelines based on the internationally recognised good practices in the area (e.g. PADIS; UN/EDIFACT; and « ICAO machine readable travel document formats »);
  - In the absence of internationally recognised good practices, it is recommended that the Commission takes a number of actions to identify the ways in which Member State could remedy to sub-optimal implementation of API systems:
    - The Frontex Advance Information Working Group could advise on ways to remedy the following issues occurring at each stage of the API data treatment and corresponding standards: data capture (effective and compliant ways of capturing API data and consistent data field requirements across systems), data transmission (best methods to transmit data manually, semi-automatically and automatically in a secure and efficient manner) and data matching (data aggregation, data cleaning and data matching to EU and national databases). In addition, this group could design frameworks for security practices (e.g. for the secure transmission, encryption, access, retention and deletion of API data) and for compliance regimes (i.e. processes to incentivise carriers compliance and common sanction regimes and guidelines)
    - The Frontex Advance Information Working Group along with Commission services could continue to regularly liaise with Working Groups from AEA, ICAO, IATA and WCO to keep abreast of the latest development, standards and good practice on advance passenger information, incorporate good practices in the follow up on emerging recommendations
    - Shall a more pressing need be identified, the EU Commission could decide to procure studies in order to conclude on good practices requiring expertise not available in the above mentioned institutions. Specific examples of such study could include: (1) a study on the extent to which existing capabilities of each port and each carrier allows for the cost-efficient, timely, automated and secure

capture and transmission of API data (2) a study on the set of optimal time windows for data transmission, which maximise security, quality and accuracy of the data taking account of carrier and third country circumstances

8.2.3 Monitoring and evaluation mechanisms and arrangements

Potential issues and related recommendations regarding the monitoring and evaluation mechanism and arrangements are:

Main issue 4:

The study evidenced the difficulties in obtaining information on the functioning of the Directive (i.e. input, output and outcomes of the implementation) and the lack of uniformity in the reporting of such data.

Recommendation 4.

It is recommended that the European Commission issue a recommendation on key indicators and statistics to be gathered to guarantee the adequate monitoring of the Directive in view its future evaluation or revision. The benefits would be to better measure the overall efficiency of the API in the future in order to also better understand the benefits of different types of API systems and whether they justify the level of investments made, both from the perspective of the carriers and the national competent authorities.

Page intentionally left blank