STUDY

Requested by the LIBE Committee

European Parliament

Advance Passenger Information (API)

An analysis of the European Commission's proposals to reform the API legal framework

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 745.768 - June 2023

EN

Advance Passenger Information (API)

An analysis of the European Commission's proposals to reform the API legal framework

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to analyse the European Commission's proposals to reform the legal framework on the processing of Advance Passenger Information (API) data. The analysis takes stock of the current legal framework regarding the processing of travellers' data. Then, it provides an outline of the Commission's proposals, followed by an assessment of the fundamental rights implications, in particular the right to respect for private life (Article 7 of the EU Charter of fundamental rights), protection of personal data (Article 8) and freedom of movement (Article 45).

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHORS

Niovi VAVOULA, Senior Lecturer in Migration and Security, Queen Mary University of London
Valsamis MITSILEGAS, Dean of the School of Law and Social Justice and Professor of European and Global Law, University of Liverpool

ADMINISTRATOR RESPONSIBLE

Alessandro DAVOLI

EDITORIAL ASSISTANT

Ivona KLECAN

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in June 2023

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
API	Advance Passenger Information
CISA	Convention Implementing the Schengen Agreement
CIR	Common Identity Repository
CJEU	Court of Justice of the European Union
CRRS	Common Repository for Reporting and Statistics
EBCG	European Border and Coast Guard
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EUDPR	European Data Protection Regulation
eu-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
FAL	Facilitation of International Maritime Traffic
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HLEG	High Level Expert Group on information systems and interoperability
iAPI	Interactive Advance Passenger Information
IATA	International Air Transport Association
ICAO	International Civil Association Organization
IT	Information Technology

LED	Law Enforcement Directive
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MID	Multiple Identity Detector
MRZ	Machine-readable Zone
NMSW	National Maritime Single Window
OSCE	Organization for Security and Co-operation in Europe
PIU	Passenger Information Unit
PNR	Passenger Name Record
RFD	Reporting Formalities Directive
sBMS	Shared Biometric Matching Service
SIS	Schengen Information System
TEC	Treaty on the European Community
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
VIS	Visa Information System
WCO	World Customs Organization

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Council Directive 2004/82/EC (API Directive) imposes obligations on air carriers to transmit, upon request, Advanced Passenger Information (API) data to the EU Member State of destination prior to the flight's take-off. API data concern biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight. The API Directive is a laconic legal instrument, implemented very differently by Member States and outdated, therefore no longer fit-for-purpose. Consequently, on 13 December 2022, the Commission adopted two legislative proposals on the collection and transfer of API data that will replace the API Directive on the obligation of carriers to communicate passenger (API) data:

- A proposal for a Regulation on the collection and transfer of API for enhancing and facilitating external border controls (API border management proposal);
- A proposal for a Regulation on the collection and transfer of API for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (API law enforcement proposal).

The proposals entail a series of amendments to the legal framework in particular:

- **Uniform rules on API data collection** including a closed and exhaustive list of API data elements, the means to collect API data, and a single point for their transfer;
- **Mandatory API data collection for the purposes of border management and combating irregular immigration on all flights entering the Schengen area;**
- **Mandatory API data collection for law enforcement purposes for all flights to and from the EU, as well as on selected flights within the EU**;
- **Better quality API data,** as air carriers will have to collect API data by automated means only;
- **Streamlined transmission of API data** by air carriers to national authorities through a new **router,** which will be developed and managed by the EU Agency for the Operational Management of Large-scale IT Systems (eu-LISA).

Aim

This study aims to provide the European Parliament with background information on the legal framework regarding the processing of API data as well as travellers' data more broadly, a legal analysis of the proposals to revise the API framework and policy recommendations so that the study can contribute to the preparation of the two legislative reports of the LIBE Committee on each of the Commission's proposals.

Key findings

The study found that the revision of the API framework takes place after the second evaluation of the API Directive in 2020, followed up by a Study supporting an Impact Assessment. Though timely, the Commission's proposals come after the adoption of the landmark judgment in *Ligue des droits humains* which provided significant limitations to the processing of Passenger Name Record (PNR) data, to which API data is a subset, and therefore the findings of the CJEU must be taken into account and be clearly echoed in the legislation. With regard to the scope of the API-related obligations, whereas the Commission's proposals adopt a sensible approach, at the heart of the assessment lies the nature and

function of the router through which the API data will be transmitted to national authorities and which will operate as a channel for information exchange and a filtering mechanism for transmitting the API data for selected intra-EU flights only, in line with *Ligue des droits humains*. The study has found that the proposed function of the router as a filtering mechanism will not be in line with the judgment, because the air carriers will transfer API data in relation to all intra-EU flights and the router will process such data in the selection process. Besides, the router may be the first step towards the forthcoming interoperability of API data with the data stored in large-scale IT systems for third-country nationals. As such, there is a heightened danger of a function creep, if in the future its operation is extended beyond the mere transmission of the API data to national authorities. The integration of API in the interoperability framework is also evident through the feeding of API data into statistics compiled by eu-LISA and the use of the technical components from the EES, ETIAS and VIS for the transfer of API data to the router. Therefore, such further use of the router is not merely hypothetical and speculative.

Whether an alternative technical solution exists is an issue that ought to have been further examined through a targeted impact assessment prior to the adoption of the API proposals, as the necessity and proportionality of the router have not been subject to a prior assessment. In any case, the development of the router should be combined with strong security standards, such as encryption of the API data, to ensure that eu-LISA does not have access to the API data transmitted and to minimise data breaches. In addition, clear assessment criteria for the collection and transfer of API data of intra-EU flights should be inserted either in the API law enforcement proposal or in a non-legislative act. These assessment criteria should not be imprecise and vague so that they can provide meaningful guidance and a methodology to the Member States in selecting intra-EU flights.

Furthermore, any extension of the scope of the API-related obligations to other modes of transport, namely sea and land carriers (railway and coaches) has already been subject to an impact assessment and it does not meet the tests of necessity and proportionality. With respect to sea carriers, reporting obligations already exist through other legal instruments. Besides, in relation to land transport the feasibility of introducing reporting obligations would disrupt the business model of carriers.

As regards the categories of API data, in particular those related to the seating and the baggage could be more precise so that the list of API data will be closed, exhaustive and precise. Furthermore, the extension of the retention period of API data (both in relation to air carriers and to border authorities) has not been justified and is not supported by the practices of the Member States in the domestic implementation of the API Directive.

In addition, the designation of eu-LISA as a data processor and not as a data controller is the legally correct assessment considering that the agency will merely provide the technical communication between the air carriers and the national authorities. In addition, from a pragmatic standpoint assigning the role of a controller to eu-LISA could create fragmentation and diffusion of responsibility and complication as to whether it is the eu-LISA or the Member States responsible for the processing of API data. The router should thus not be used as a means for Member States to evade their data protection responsibilities.

Other data protection-related provisions of the proposals must be clarified, including the exercise of individual (data protection) rights enjoyed by travellers and the supervision of air carriers as the proposed rules are unclear. Finally, the proposals should include additional safeguards regarding the use of the statistical data retrieved from the Common Repository for Reporting and Statistics (CRRS) by eu-LISA. These safeguards are necessary to ensure that the statistical data will not be used for risk analysis, profiling or predictive risk assessment, which may be detrimental to travellers who may be subject to discriminatory treatment.

1. INTRODUCTION

1.1. Background

Since the past few decades, travelling by air has drastically increased; according to the International Civil Aviation Organization (ICAO) in 2019 4.5 billion passengers were globally carried by air transports on scheduled services.[1] In 2023, it is forecasted that air passenger demand will rapidly recover to pre-pandemic levels on most routes by the first quarter and that growth of around 3% on 2019 figures will be achieved by the end of the year.[2] It is also noted that every year, **over a billion passengers** enter, leave or travel within the EU.[3]

Advance Passenger Information (API) is commonly understood as the information of an air passenger collected at check-in at the airport or at the time of online check-in. API includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight. The processing of API data has been considered as an effective tool for advance checks of air passengers, allowing to expedite procedures upon arrival and allocating more resources and time to identify travellers who need further attention.[4]

At EU level, Council Directive 2004/82/EC (API Directive) imposes obligations on air carriers to transmit, upon request, API data to the EU Member State of destination prior to the flight's take-off.[5] The API Directive has been in force since September 2006 and has subsequently been evaluated twice; in 2012[6] and 2020,[7] revealing wide discrepancies in national implementations coupled with additional concerns regarding the out-of-date character of the legislative framework given that in the meantime Directive 2016/681 on the processing of Passenger Name Record (PNR) data,[8] which is closely linked to API – the latter is a subset of PNR – and data protection framework has been modernised through the adoption

[*] The authors are grateful to Gregory Slevin for proofreading this study and Elif Mendos Kuskonmaz for valuable insights into the application of the PNR requirements in practice.

[1] ICAO, 'The World of Air Transport in 2019' https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx accessed 27 April 2023.

[2] ICAO, 'ICAO forecasts complete and sustainable recovery and growth of air passenger demand in 2023' (8 February 2023) https://www.icao.int/Newsroom/Pages/ICAO-forecasts-complete-and-sustainable-recovery-and-growth-of-air-passenger-demand-in-2023.aspx accessed 27 April 2023.

[3] 'Security Union: Commission proposes new rules on Advance Passenger Information to facilitate external border management and increase internal security' (13 December 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7644 accessed 27 April 2023.

[4] Commission, 'Staff Working Document – Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)' SWD(2020) 174 final (2020 Evaluation of API Directive), 10.

[5] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data [2004] OJ L262/24 (API Directive).

[6] Commission, Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82' (2012).

[7] Commission, 'Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data' (2020).

[8] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ 119/132 (PNR Directive).

of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR),[9] Directive 2016/680 (Law Enforcement Directive – LED)[10] and Regulation 2018/1725 (EU Data Protection Regulation – EUDPR).[11]

In its Schengen Strategy of June 2021, the Commission presented its Communication 'A strategy towards a fully functioning and resilient Schengen area', which stressed the need for an increased use of API data in combination with PNR data to significantly enhance internal security in line with fundamental rights and free movement.[12] Against this backdrop, on 13 December 2022, the Commission adopted two legislative proposals on the collection and transfer of API data that will replace the API Directive on the obligation of carriers to communicate passenger (API) data:

- A proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of API for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 (Interoperability Regulation for border checks)[13] and Regulation (EU) 2018/1726 (eu-LISA Regulation),[14] and replacing the API Directive (API border management proposal);[15]
- A proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of API for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2018/818 (Interoperability Regulation for law enforcement)[16] (API law enforcement proposal).[17]

In a nutshell, the proposed rules on API will entail the following main amendments:

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OH 119/1 (GDPR).

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (LED).

[11] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) [2018] OJ L295/39 (EUDPR).

[12] Commission, 'A strategy towards a fully functioning and resilient Schengen area' (Communication) COM(2021) 277final.

[13] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L135/27 (Interoperability Regulation for border checks).

[14] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 [2018] OJ L295/99 (eu-LISA Regulation).

[15] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC' COM(2022) 729 final (API border management proposal).

[16] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L135/85 (Interoperability Regulation for law enforcement).

[17] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818' COM(2022) 731 final (API law enforcement proposal).

- **Uniform rules on API data collection:** The new rules include a closed and exhaustive list of API data elements, the means to collect API data, and a single point for their transfer;
- **Mandatory API data collection for the purposes of border management** and combating irregular immigration on all flights entering the Schengen area;
- **Mandatory API data collection for law enforcement purposes** for all flights to and from the EU, as well as on selected flights within the EU;
- **Better quality API data,** as air carriers will have to collect API data by automated means only;
- **Streamlined transmission of API data** by air carriers to national authorities through a new **router,** which will be developed managed by the EU Agency for the Operational Management of Large-scale IT Systems (eu-LISA).

1.2. Aim of the study

Against this backdrop, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) has requested a study on API that will contribute to the preparation of two LIBE forthcoming legislative reports on this matter, as well as to the subsequent negotiations with the Council. The study's objective is to provide the European Parliament with background information on API's current legal framework, including its relationship with PNR-related requirements and a legal analysis of the Commission's proposals to reform the API framework. The proposals are analysed from the perspective of fundamental rights, as enshrined in the EU Charter of Fundamental Rights (Charter), particularly the rights to respect for private life (Article 7), the right to the protection of personal data (Article 8) and freedom of movement (Article 45). The study also offers concluding remarks and policy recommendations.

1.3. Methodology

This study is based on desk research and the review of existing available data, reports, studies and analyses from various sources and documents primarily from EU and international institutions, agencies and bodies, as well as academia and civil society. It principally encompasses legal instruments and policy documents of EU institutions, bodies and agencies, such as Council documents examining aspects of the proposal, resolutions of the European Parliament and opinions by the European Data Protection Supervisor (EDPS). An analysis of EU primary and secondary legislation from the perspective of fundamental rights, as interpreted in the jurisprudence of the Court of Justice of the European Union (CJEU), is central to this research. The desk research has been complemented by informal discussions with Officials from the EDPS and the EU Agency for Fundamental Rights (FRA). Where their input has been incorporated in the text, this is clearly indicated. In view of the ongoing examination of the proposals within the Council, the analysis is updated until 27 April 2023, taking into account to the extent possible all relevant documentation, including Council documents.

1.4. Structure

This study is structured as follows: Section 2 provides a concise sketch of the current legal framework on processing API and Passenger Name Record (PNR), including its implementation at national level, so as to inform the subsequent analysis. The section outlines the relevant case law of the CJEU on the processing of PNR data, in particular the judgment in Case C-817/19 *Ligue des droits humains*, released in June 2022.[18] Section 3 provides an outline of the proposals amending the API legal framework. Section 4 is dedicated to the legal assessment of the proposals in light of the protection of fundamental rights, especially the rights to respect for private life (Article 7 of the EU Charter of Fundamental Rights) and protection of personal data (Article 8). In particular, the study examines the compatibility of the proposed rules (including their potential reformulation in the Council) with the aforementioned rights in respect of the following aspects: the scope of the proposed rules, the categories of API data processed, the development of the router, individual rights, supervision and the forthcoming interoperability of API data with information systems. Other aspects of broader interest under EU law are also examined. The study concludes with an overall assessment of the proposals, as well as policy recommendations for relevant actors.

[18] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministers* ECLI:EU:C;2022:491.

2. PROCESSING OF TRAVELLERS' DATA UNDER EU LAW

The establishment of systems for the collection and transfer of API data is an international standard. At international level, the main regulatory instruments on the use of the API data are the WCO/IATA/ICAO API Guidelines from 2022[19] and Annex 9 of the Convention on International Civil Aviation (Chicago Convention) to which all Member States are parties.[20] In recent years, calls for maximising the use of API and PNR data particularly in the framework of using that data for the screening of travellers have been reinforced: the United Nations (UN) Security Council Resolutions has issued numerous resolutions (2178(2014),[21] 2309(2016),[22] 2396(2017),[23] 2482(2019).[24] calling for the establishment and global roll-out of API and PNR systems to detect departures or attempted entry or transit of suspects to counter terrorism. Furthermore, in 2016, the participating states to the Organization for Security and Co-operation in Europe (OSCE) issued a Ministerial Council Decision on enhancing the use of API.[25] Moreover, in 2017, the leaders at the G7 issued a statement on the fight against terrorism and violent extremism, focusing on the expansion of the use of PNR and API data in screening passengers. The importance of filling gaps in the use of API data at international level was reiterated as an effective instrument in the fight against terrorism.[26]

2.1. Air carriers: API and PNR

2.1.1. API Directive in a Nutshell

Council Directive 2004/82/EC (API Directive) regulates the collection and transmission of API data in the 30 implementing countries (EU Member States and three Schengen Associated States).[27] This Schengen legal instrument is legally based on Articles 62(2)(a) and 63(3)(b of the Treaty on the European Community (TEC), therefore it is a border management tool. It obliges air carriers to transmit, upon request of the authorities responsible for carrying out checks on persons at external borders, passenger data to the Member State of destination by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will

[19] The API Guidelines were initially developed in 1993 by the World Customs Organization (WCO) in cooperation with the International Air Transport Association (IATA). Subsequently, the International Civil Aviation Organization (ICAO) joined the process and a 'Contact Committee' comprising of the three organisations was formed. In order to help their respective members, implement the API system, the three organisations have jointly published the WCO/IATA/ICAO Guidelines on Advance Passenger Information in 2003, 2010, 2013 and more recently in 2022. See https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx accessed 27 April 2023.

[20] Convention on International Civil Aviation (Chicago Convention) signed in 1944.

[21] UN Security Council, Resolution 2178(2014) (24 September 2014).

[22] UN Security Council, Resolution 2309(2016) (22 September 2016).

[23] UN Security Council, Resolution 2396(2017) (21 December 2017).

[24] UN Security Council, Resolution 2482(2019) (19 July 2019).

[25] OSCE, 'Ministerial Council Decision 6/16 of 9 December 2016 on Enhancing the use of Advance Passenger Information' https://www.osce.org/cio/288256 accessed 27 April 2023.

[26] European Council, 'G7 Taormina Statement on the fight against terrorism and violent extremism' (26 May 2017) https://www.consilium.europa.eu/en/press/press-releases/2017/05/26/statement-fight-against-terrorism/ accessed 27 April 2023.

[27] The United Kingdom participated in the API Directive, in accordance with Recital 15 of the API Directive, but is no longer subject to these requirements following Brexit. The Trade and Cooperation Agreement refers to the processing of PNR data. Liechtenstein is bound by the Schengen *acquis* but does not have an airport.

enter the territory of a Member State.[28] The primary objective of the API Directive is to improve border control and combat irregular migration,[29] however Article 6 allows the use of API data for law enforcement purposes in accordance with national law.[30]

The API Directive mandates the transfer of the following information: the number and type of travel document used; nationality; full names; 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.[31] Member States must ensure that the data are collected by the carriers and transmitted electronically, or in case of failure, by any other appropriate means to the border authorities, which must save the data in a temporary file.[32] The retention period of the data is 24 hours from transmission, unless the data are needed later for the purpose of exercising statutory functions of the authorities responsible for carrying out checks on persons at external borders.[33] Similarly, the carriers must delete the data within 24 hours of the flight's arrival.[34] Member States must take the necessary measures to impose dissuasive, effective and proportionate sanctions on carriers which, as a result of fault, have not transmitted data or have transmitted incomplete or false data.[35] These sanctions must be either the maximum amount is not less that 5,000 euros, or the minimum is not less than 3,000 euros per journey. Member States are not prevented from imposing other sanctions, such as immobilisation, seizure and confiscation of the means of transport, or temporary suspension or withdrawal of the operating licence for very serious infringements.[36] According to Article 6(2) individuals enjoy the right of information.

Overall, the API Directive is a fairly laconic legal instrument; it only sets minimum standards for the Member States to request API data and Member States are free to also request similar information in respect of other means of transport, such as maritime or rail transport carriers.[37] Attention should also be drawn to the wording of Recital 9, which states that [i]n order to combat illegal immigration more effectively and in order to ensure the greater effectiveness of this objective, it is essential that […] account be taken at the earliest opportunity of any technological innovation, especially with reference to the integration and use of biometric features in the information to be provided by the carriers. This wording therefore hints towards the shape a future reform of the legal framework may take.

2.1.2. (Problematic) implementation of the API Directive

The deadline for transposing the API Directive was the 5th September 2006. Two evaluations have taken place; in 2012[38] and 2020.[39] The latter found, that in 2019, when the study was carried out, 25 out of the

[28] API Directive, art 3. For an analysis see Valsamis Mitsilegas, 'Contrôle des Etrangers, des Passagers, des Citoyens: Surveillance et Anti-terrorisme' (2005) 20 *Cultures & conflits* 185.

[29] API Directive, art 1.

[30] Ibid, art 6(1) last subparagraph.

[31] Ibid, art 3(2).

[32] Ibid, art 6(1).

[33] Ibid.

[34] Ibid.

[35] Ibid, art 4.

[36] Ibid.

[37] Ibid recital 8.

[38] See n 6.

[39] See n 7.

then 32 participating States that had functioning API systems in place, two Member States were in pilot phase[40] and another four were planning to introduce an API system by 2020.[41]

Whereas the evaluation concluded that the API Directive has been adequately transposed, most of its articles presented conformity assessment issues, to a large extent attributed to the fact that the API Directive sets only limited criteria for the collection, transmission and processing of API data. Overall, Slovenia is the only Member State in full conformity with the Directive.[42] There is a diversity of API systems in the EU notably due to the different national legislations and organisational structures. Some API systems are centralised under one unit, while others are set up in a decentralised manner.[43]

On average, for all Member States combined, it is estimated that API data are collected on 65% of inbound flights,[44] which may enable individuals who want to avoid checks to bypass routes where API data are consistently collected and instead travel to their destination via flights routers where API data are often or not at all processed.[45] With regard to the objectives pursued by the API system half of the Member States have gone beyond the purposes foreseen by the Directive to encompass additional ones.[46] The definitions laid down in the Directive have also not been fully transposed by 13 Member States.[47] Moreover, the list of data elements contained in the API Directive is non-exhaustive and Member States can request additional data elements pursuant to national law.[48] In addition, the legal framework does not take into account the evolution of international standards, particularly the WCO//IATA/ICAO guidelines on API from 2013.

With regard to the use of API for law enforcement purposes, the implementation of this possibility is patchy, raising security concerns due to the lack of standardised and uniform criteria on the collection and transfer of API data for law enforcement purposes and the parallel application of the PNR Directive. A more detailed account on the use of API data for law enforcement purposes is provided in a previous Study for the LIBE Committee.[49] For the purposes of providing a holistic approach a summary of these findings is hereby provided. In a nutshell, with the exception of the Netherlands and Slovenia, all other participating States have made use of this discretion.[50] Member States are using API data for law enforcement purposes in different ways: to match API data against national counter-terrorism and

[40] These are: Belgium and Slovakia.

[41] These are: Cyprus, Greece, Iceland, and Norway.

[42] Commission, 'Study on Advance Passenger Information (API)' (n 6) 30.

[43] European Border and Coast Guard Agency (EBGA) 'Report on API Systems and Targeting Centres (2018).

[44] Commission, 'Commission Staff Working Document – Impact Assessment Report accompanying the documents "Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC" "Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818"'SWD(2022) 422final, 7. There is an estimated use of API data for 25 % of all outbound flights for law enforcement purposes under national law. Ibid.

[45] Commission, 'API border management proposal' (n 15) 1.

[46] Commission, 'Study on Advance Passenger Information (API)' (n 6) 30-31.

[47] Ibid.

[48] Ibid 39-41.

[49] Niovi Vavoula, 'Police Information Exchange – The future development regarding Prüm and the API Directive' (Study commissioned by the LIBE Committee of the European Parliament, 2020).

[50] Commission, 'Study on Advance Passenger Information (API)' (n 6) 35. In 21 Member States API data are being used for the purposes of law enforcement (Ibid, 183. These are: Austria, Belgium, Switzerland, Czech Republic, Denmark, Estonia, Greece, Spain, France, Croatia, Latvia, Lithuania, Slovakia, United Kingdom, Romania, Finland, Iceland, Germany, Cyprus and Luxemburg); and in 15 for fight against terrorism (Austria, Belgium, Czech Republic, Denmark, Estonia, Greece, France, Croatia, Latvia, Lithuania, Sweden, Slovakia, United Kingdom, Germany and Cyprus).

counter-organised crime databases; comparing API data against the SIS, including alerts on discreet checks; matching against foreign counter-terrorism databases;[51] and processing of API data jointly with PNR to match risk profiles and criteria for the purposes of identifying possible criminal behaviour or participation in terrorist acts - in this process, the API data is primarily used to verify the PNR-based analysis and profiling. The API data is rarely, if at all, used to match pre-defined risk profiles.[52]

Other issues that have emerged are the following: first, the lack of a definition of what 'law enforcement' purposes may encompass, with national implementation at the national level going beyond the material scope of the PNR Directive and varying from enhancing internal security and public order, to fight against terrorism and national security.[53] Second, the API data elements do not entirely match in both Directives, notably due to the non-exhaustive list of API data in the API Directive.[54] Third, the two instruments do not apply to the same type of flights, as the API Directive does not prescribe the collection of API data for intra-EU flights.[55] Fourth, the API Directive does not foresee a data retention period for the use of API data for law enforcement purposes and this issue is left for determination in national laws; the 24-hour limit is only in connection to their use for border control purposes. [56]

In order to reconcile these two instruments, the study proposed the establishment of what is referred to as the 'single window' model to receive both API and PNR data,[57] as well as 'targeting centres' to receive all forms of passenger data in one single entry point. Through a 'targeting centre,' a Member State may conduct risk assessment of travellers based on personal data stemming from different sources (such as EU information systems and API data) through 'tactical risk analysis' in order to detect unknown persons of interest before they come to the border.[58] The study noted that 13 Member States use the 'single window' model, according to which API data are sent to the Passenger Information Unit (PIU) by the push method, which typically acts as the targeting centre.[59]

Overall, this loose legal framework leads to very diverging practices at the national level, which undermines the effectiveness of the Directive and creates a burden on air carriers which must comply with differing requirements depending on the routers and the Member State requesting API data.[60] Additional discrepancies are also evident as a result of the adoption of new legislation on border management, such as the legal instruments on EU information systems, passenger information, namely the PNR Directive, discussed below, and the general legal instruments in EU data protection law,

[51] Ibid, 73. Two Member States (Bulgaria and Italy) have reported on such use, although others are likely to match data against major databases maintained by the United States as well.

[52] Ibid 73.

[53] Ibid, 56.

[54] Ibid 62. The PNR Directive provides for different API data elements than API Directive, stating '(a)ny advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)'. For example, gender is not a mandatory API data element in the API Directive.

[55] Ibid.

[56] A majority of Member States apply the provisions of the PNR Directive, (also due to the joint collection of API and PNR data). Ibid 51.

[57] According to ICAO93, the 'single window' concept should apply to each form of passenger data that an airline is obliged to transmit to the requesting authority, i.e. Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR).

[58] Commission, 'Study on Advance Passenger Information (API) (n 6) 39.

[59] Ibid.

[60] Commission, 'API border management proposal' (n 15) 2.

namely GDPR, the LED and the EUDPR. The new international standards and calls for further exploitation of API data are also factors necessitating the revision of API rules.

2.1.3. The PNR Directive

When a passenger buys a ticket with an air carrier, a PNR is generated by the reservation systems of air carriers for their business purposes, which includes data not only on the complete itinerary, but also information on the seat reserved, weight of the luggage, frequent flyer status, payment details, contact details and special requests of passengers (such as meal options or special assistance requests). Because of the variety of information contained in the PNR, it is deemed valuable for uncovering and confirming passengers' travel and behavioural patterns and for identifying high-risk travellers.[61]

PNR data and API are closely linked; in its definition, PNR data include 'any advance passenger information (API) data collected'.[62] When used together they are considered as particularly effective in identifying high-risk travellers and confirming the travel pattern of suspected individuals. However, the PNR Directive does not oblige air carriers to collect any data beyond the normal course of business, which means that the PNR Directive does not lead to the collection of the full set of API data, as air carriers 'do not have any business purpose to collect such data'.[63] The main differences between API and PNR data are the following: API data are mainly used as an identity verification and border management tool. This is because API data do not enable law enforcement authorities to conduct a risk assessment of passengers, and therefore do not facilitate the detection of 'unknown' criminals or terrorists.[64] Importantly, whereas API data are considered as information of 'typically verified nature', as it concerns the passengers that have eventually boarded a plane and because it corresponds to biographical information about passengers captured from their travel documents, PNR data constitute 'unverified' information provided by passengers when booking their flight. Therefore, the reliability of API data is much higher, however it is acknowledged that the data may be incomplete and incorrect due to the growing reliance on online check-in where passengers self-declare their data.

The PNR Directive concerns the use of PNR data for the prevention, detection, investigation and prosecution of terrorism offences and serious crimes.[65] Therefore, the primary purpose of the API Directive is border control and the fight against irregular migration, whereas the PNR Directive pertains to law enforcement. The PNR Directive places a duty on airline carriers operating international flights between the EU and third countries to forward PNR data of all passengers to the Passenger Information Unit (PIU) established at domestic level for this purpose. Member States are given the discretion to extend the regime set out in the Directive to intra-EU flights, even to a selection of them.[66] Unsurprisingly, on 18 April 2016 Member States declared in a statement that they intended to make full use of the possibility provided for in the Directive of requiring PNR on intra-EU flights.[67] All Member States but one have notified the Commission on the collection of PNR data in intra-EU flights under Article 2 States have declared their intention to make use of their discretion. The PNR-related

[61] Commission, 'API law enforcement proposal' (n 17) 1.

[62] PNR Directive. Annex I, point 18.

[63] Commission, 'API law enforcement proposal' (n 17) 13.

[64] Commission, 'Commission Staff Working Document – Impact Assessment Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime' COM(2011) 132final.

[65] PNR Directive, art 1.

[66] Ibid art 2.

[67] Council, Document 7829/16 (18 April 2016).

obligations concern terrorism, as defined in Directive 2017/541[68] and serious crime, as listed in Annex II of the PNR Directive, provided that the offences are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.[69]

Once transmitted, the data are stored and analysed by the national PIU to identify persons who were previously unsuspected of involvement in terrorism or serious crime[70] and require further examination by competent authorities in relation to those offences listed in Annex II of the Directive. PNR data are used in different ways – real-time, by assessing incoming and outgoing passengers for further examination before their flights; reactively on a case-by-case basis to respond to inquiries from national competent authorities in preventing, detecting, investigating and prosecuting terrorism offences and serious crimes, and pro-actively to update or create new criteria for real-time assessment of passengers.[71] For real-time processing of PNR data, PIUs may compare the data against databases including those on persons or objects sought or under alert, or so-called pre-determined criteria,[72] which must be targeted, proportionate and specific, regularly reviewed and not based on protected characteristics of individuals.[73]

The initial retention period is six months, after which PNR data are depersonalised, meaning that the PIU is entrusted with the task of masking out the names, address and contact information, payment information, frequent flyer information, general remarks, and all API data.[74] They may still be used for criminal law purposes under 'very strict and limited conditions'[75] – that is, if so permitted by a judicial authority or another national authority competent to review whether the conditions have been met and subject to information and ex post review by the Data protection Office of the PIU.[76]

In 2020, the PNR Directive was also subject to evaluation, where the Commission found that though the added value of processing PNR data based on qualitative evidence (e.g. routes or travel agencies previously used by human traffickers), there exist challenges regarding the reliability and completeness of PNR data that may lead to false positive matches. A way forward to address these challenges is to ensure that more PNR data are transferred to PIUs and to process PNR data jointly with the more reliable API data.

Contrary to the API Directive that has not received much scholarly attention, the PNR Directive has been criticised based on fundamental rights concerns, particularly in relation to the protection of privacy, data protection and free movement rights.[77] Issues of interest are the extent to which the bulk processing of PNR data of all individuals taking flights, who are unsuspected of criminal activity constitutes unlawful generalised and indiscriminate surveillance, as proclaimed by the CJEU in its

[68] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

[69] PNR Directive, art 3(9).

[70] Ibid recital 7.

[71] Ibid art 6.

[72] Ibid art 6(3).

[73] Ibid art 6(4).

[74] Ibid art 12.

[75] Ibid recital 25.

[76] Ibid art 12(3).

[77] Elif Mendos Kuskonmaz, 'PNR Directive' in Violeta Moreno-Lax and Niovi Vavoula (eds), *Oxford Encyclopedia of European Union Law – Area of Freedom, Security and Justice* (Oxford University Press, forthcoming 2023); Niovi Vavoula, 'The EU Response to the Phenomenon of Foreign Fighters: Challenges for Fundamental Rights and the Rule of Law' in Ulrich Sieber et al. (eds), *Alternative, Informal, and Transitional Types of Criminal Justice and the Legitimacy of New Sanction Models in the Global Risk Society* (Duncker & Humblot 2018); Maria Tzanou, The Fundamental Right to Data Protection -Normative Value in the Context of Counter-terrorism Surveillance (Hart 2017).

jurisprudence on data retention regimes under EU law. The risks regarding profiling of travellers through their prior assessment, including against algorithms (the pre-determined criteria) are also central in this debate, not least due to the significant margin of error resulting from automated profiling.

2.1.4. The PNR Directive in the jurisprudence of the CJEU

In June 2022, the CJEU released its judgment in Case C-817/19 *Ligue des Droits Humains* concerning the compatibility of the EU PNR Directive with the right to respect for private life and the right to personal data protection, enshrined in Articles 7 and 8 of the Charter.[78] This is the first of several requests for preliminary rulings regarding the compatibility of the PNR Directive with the Charter.[79] Prior to that judgment, the CJEU had the opportunity to assess the processing of PNR data in Opinion 1/15 regarding the compatibility of the draft EU-Canada agreement on PNR data transfers.[80]

The CJEU confirmed the validity of the PNR Directive, but provided a series of limitations on the processing of personal data to ensure compliance with the rights to respect for private life and protection of personal data.[81] Among its many pronouncements, the CJEU provided a strict interpretation on which PNR data elements as listed in Annex I of the PNR Directive may be processed.[82] Furthermore, with regard to the definition of serious crime, the CJEU provided a minimum three-year imprisonment requirement to exclude ordinary crimes[83] and required that PNR data are processed for only those serious crimes that have an objective link including an indirect one with the carriages of passengers.[84] On the applicability of the PNR to intra-EU flights, the Court found that it can only be applied to such flights in situations other than a terrorist threat, relating to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application and this extension should be based on a prior assessment by the Member States ensuring that such extension is strictly necessary.[85]

Additional limitations were provided in connection to the automated processing of PNR data by PIUs; the databases against which the data are cross-checked must be limited to non-discriminatory databases,[86] used for the fight against terrorism and serious crime.[87] Furthermore, the use of pre-determined criteria means that the use of artificial intelligence technology in self-learning systems ('machine learning') capable of modifying without human intervention or review, the assessment

[78] *Ligue des Droits Humains* (n 18).

[79] C-148/20 *AC v Deutsche Lufthansa AG*, OJ C 279/21; C-149/20 *DF v Deutsche Lufthansa SA*, OJ C279/21; C-150/20 *BD v Deutsche Lufthansa SA*, OJ C279/22; C-215/20 *JV v Bundesrepublik Deutschland*, OJ C 279/27; C-222/20 *OC v Bundesrepublik Deutschland*, OJ C 279/30; C-486/20 *Varuh človekovih pravic Republike Slovenije*, OJ C414/24.

[80] Opinion 1/15 ECLI:EU:C:2017:592. For an analysis see among others Anna Vedaschi, 'The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017' (2018) 14 *European Constitutional Law Review* 410; Elif Mendos Kuskonmaz and Elspeth Guild, 'EU exclusive jurisdiction on surveillance related to terrorism and serious transnational crime, case review on opinion 1/15 of the CJEU' (2018) 43 *European Law Review* 583.

[81] For analysis of the judgment see Evelien Brouwer, '*Ligue des Droits Humains* and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in times of new technologies' (Common Market Law Review, forthcoming 2023); Christian Thonnes, 'A Directive Altered beyond Recognition - On the Court of Justice of the European Union's PNR decision (C-817/19)' (*Verfassungblog*, 23 June 2023) https://verfassungsblog.de/pnr-recognition/ accessed 27 April 2023.

[82] *Ligue des Droits Humains* (n 18) paras 130-136.

[83] Ibid para 151.

[84] Ibid para 156.

[85] Ibid paras 168-174.

[86] Ibid para 190.

[87] Ibid para 191.

criteria as well as the weighting of those criteria is precluded.[88] To address challenges regarding the prohibition of non-discrimination, including both direct and indirect discrimination, the CJEU has imposed additional requirements on algorithmic profiling adding to those mentioned in Opinion 1/15.[89]

In addition, the procedural requirements for authorising access to PNR data after the first six months until the end of the five-year retention period must also be applicable during the first six months from its initial collection by the PIUs.[90] Designating the PIUs as the authorising body would not satisfy the independence requirement; as authorities competent for the prevention, detection, investigation, and prosecution of terrorist offences and serious crimes, they are involved in criminal proceedings and cannot take a neutral stance.[91] A general retention period of five years for PNR data, applicable indiscriminately to all air passengers is also prohibited.[92]

Finally, the CJEU partly dealt with the API Directive, as the Belgian legislation implementing the PNR Directive, the legality of which was at stake, required the processing of PNR and API in relation to all flights, including intra-EU flights and other modes of transports both for purposes related to external border checks and combating irregular migration and law enforcement purposes. The Court found that:

> 'A measure whereby a Member State would extend the provisions of the API Directive, for the purposes of improving border controls and combating illegal immigration, to intra-EU and, a fortiori, other modes of transport carrying passengers within the European Union departing from, going to or transiting through that Member State, in particular the obligation to provide the data covered by Article 3(1) of that directive, would amount to allowing the competent authorities, when internal borders of the said Member State are crossed, to ensure systematically that those passengers can be authorised to enter its territory or to leave it and would thus have an effect equivalent to the checks carried out at external borders with third countries.'[93]

2.2. Sea carriers

Obligations for maritime carriers to collect and transfer personal data of passengers and crew derive from the Schengen Borders Code.[94] In particular, Annex VI of the Schengen Borders Code states that information on the crew and passengers must be transmitted by sea carriers to border authorities, or if national law so provides, to other relevant authorities. The data must be transmitted as a list containing the information laid down in the FAL form 5 (crew list) and FAL form 6 (passenger list) of the Convention on Facilitation of International Maritime Traffic (FAL Convention), as well as, where applicable, visa or residence permit numbers.[95] The information must be communicated at the latest twenty-four hours

[88] Ibid para 194.

[89] Opinion 1/15 (n 80) paras 168-174. A person must be able to understand how risk assessment criteria and programs work, to allow him or her to decide with full knowledge of the relevant facts whether or not to claim the unlawful and indiscriminatory nature of these criteria. Ibid para 201).

[90] Ibid paras 222-228.

[91] Ibid paras 244-245.

[92] Ibid para 262.

[93] Ibid para 288.

[94] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) [2016] OJ L77/1, as amended.

[95] Also see Article 26 of the Convention Implementing the Schengen Agreement (CISA) provides that air, sea and international carriers transporting groups overland by coach are obliged to assume responsibility for any travellers who

before arriving in the port, or at the latest at the time the ship leaves the previous port, if the voyage time is less than twenty-four hours, or if the port of call is not known or it is changed during the voyage, as soon as this information is available. The information on crew and passengers required by the FAL forms is not the same as that laid down in the API Directive; for example, the gender of the individual is collected, as well as additional information on the travel document.[96]

Specific obligations to collect passenger information (passenger manifests) with regard to ferry connections with ports situated in third countries were first introduced by Directive 98/41/EC (PAX Directive) on the registration of persons sailing onboard passenger ships operating to or from ports of the Member States,[97] as amended several times, with the latest amendment being by Directive 2017/2109.[98] The latter provides that a passenger ship should record the family name of each person on board, their forename(s), gender, nationality, date of birth and, if provided by the passenger, a contact number in case of an emergency, as well as information concerning special care or assistance that might be needed in an emergency.[99]

Additional rules were provided by Directive 2002/6/EC,[100] repealed by Directive 2010/65/EU (Reporting Formalities Directive (RFD).[101] The latter prescribes that the reporting formalities (forms 5 and 6) should be transmitted electronically via the National Maritime Single Window (NMSW). Article 4 provides for the prior notification of at least 24 hours of arrival into ports situated in a Member State, including the passenger list. Member States are obliged to establish NMSWs for reporting formalities from ships arriving and/or departing from ports. Following the Council's 'Valetta Declaration' of 2017, calling for the digitalisation and administrative simplification of the maritime sector, Regulation (EU) 2019/1239, that will replace Directive 2010/65/EU from August 2025.[102] The Regulation establishes a European Maritime Single Window and aims to harmonise the interfaces available to ships' operators to provide information and to create a standardised maximum dataset.

2.3. Land carriers (railways and coaches)

Under EU law, there are no obligations for land carriers, such as rail or coach companies to collect and transfer API data from passengers. Extension of such requirements to land carriers has taken place on an ad hoc and limited basis by some Member States when implementing the API Directive. In particular, the Commission's evaluation report states that in four Member States API data are collected from

are refused entry. Furthermore, with regard to air and sea travellers, they must take all necessary measures to ensure that they are in possession of the travel documents required for entry.

[96] Commission, 'Study supporting an impact assessment: potential effects of different possible measures on Advance Passenger Information' (2021) 19.

[97] Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community [1998] OJ L188/3.

[98] Directive (EU) 2017/2109 of the European Parliament and of the Council of 15 November 2017 amending Council Directive 98/41/EC on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community and Directive 2010/65/EU of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States [2017] OJ L315/52.

[99] Ibid art 5.

[100] Directive 2002/6/EC of the European Parliament and of the Council of 18 February 2002 on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community (Text with EEA relevance) [2002] OJ L67/31.

[101] Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC Text with EEA relevance [2010] OJ L283/1.

[102] Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU [2019] OJ L198/64.

railway companies, namely Estonia, France, Finland and the United Kingdom (prior to Brexit), whereas only in Austria API data are collected from coaches/buses.

2.4. Interoperable databases for checks of travellers at EU's external borders

The aforementioned requirements under EU (and national) law must be considered in conjunction with recent developments on the implementation of other tools relevant to border management which are currently in the pipeline, namely the Entry/Exit System (EES), the Visa Information System (VIS) and the European Travel Information and Authorisation System (ETIAS).[103] It is beyond the scope of this study to provide a detailed outline of the legal framework governing the large-scale IT systems in the EU Area of Freedom, Security and Justice (AFSJ). Therefore, this sub-section will merely provide a concise sketch to inform the subsequent analysis. This is because, as it will be explained below and in the next Chapters, the API proposals place the revision of the API legal framework within the broader framework of the forthcoming operationalisation of additional large-scale IT systems for third-country nationals.

The EES, the legal basis of which is Regulation 2017/2226,[104] will register the border crossings, both at entry and exit, of all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.[105] EES is a multi-purpose tool: it aims to enhance the efficiency and automation of border checks, assist in the identification of irregular migrants and overstayers, combat identity fraud and misuse of travel documents and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.[106]

The VIS, operational since 2011, but subject to revised rules currently under implementation, stores a wide range of personal data (both biographical and biometric) on individuals applying for short-stay (Schengen) visas as well as long-stay visas and residence permits.[107] The VIS is also a multi-purpose tool aimed at improving the implementation of the common visa policy, with numerous sub-purposes envisaged, including the fight against fraud and visa shopping and the contribution to the prevention of threats to Member States' internal security.

The ETIAS, set up by Regulation (EU) 2018/1840, will apply to third-country nationals who are exempt from the requirement to be in possession of a Schengen visa when crossing the external borders of the EU.[108] Its purpose is to identify whether their presence in the territory of the Member States would pose a security, irregular migration or high epidemic risk.[109] In order to assess these risks, the ETIAS

[103] For a detailed account on large-scale IT systems for third-country nationals see Niovi Vavoula, *Immigration and Privacy in the Law of the European Union – The Case of Information Systems* (Brill 2022).

[104] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L327/20 (EES Regulation).

[105] Subject to certain exceptions. See EES Regulation, art 2(3).

[106] Ibid art 6(1).

[107] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2018] OJ L218/60 (VIS Regulation).

[108] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L236/1 (ETIAS Regulation).

[109] Ibid art 1.

Regulation prescribes that all visa-exempt third-country nationals will be required to apply online for travel authorisation prior to the date of their departure. In processing each application, the system will automatically compare the personal data submitted by the applicants with the data in the EU and certain international databases and against screening rules.[110]

The establishment of an elaborate legal framework governing the EU information systems has been complemented by efforts to enable the systems 'speak to each other' and the interaction of data from different sources in various ways. The Interoperability Regulations 2019/817 and 2019/818 adopted on 20 May 2019 prescribe four main components, which are currently developed by eu-LISA with the aim of becoming operational in 2024: a European Search Portal (ESP) that will enable competent authorities to simultaneously query the underlying systems and the combined results will be displayed on a single screen;[111] a shared Biometric Matching Service (sBMS) that will generate and store templates from all biometric data recorded in the underlying systems;[112] a Common Identity Repository (CIR) that will store an individual file for each person registered in the systems, containing both biometric and biographical data;[113] and a Multiple Identity Detector (MID) that will use the alphanumeric data stored in the CIR and the SIS to detect multiple identities.[114] Statistical data will be compiled through the Central Repository for Reporting and Statistics (CRRS).[115]

The linkages between the API data and the interoperable databases have long been hinted in various documents: in 2017, the High Level Expert Group on information systems and interoperability (HLEG) stated that in the future an interactive API data will be necessary to enable carriers to check a travel authorisation and to check remaining authorised stay (EES & VIS) in the absence of stamps in the passport. This exchange will need to take place between all airlines and the EES/ETIAS central system.[116]

With API data deemed as an important tool for facilitating border control as it allows for faster clearance of passengers, another key question emerges: what is the role of API data in the emerging interoperability framework? In its Communication on Stronger and Smarter Information Systems for Borders and Security, the Commission emphasised that in line with existing best practice, Member States should increase the added value of API by establishing automated cross-checking against SIS and Interpol's Stolen and Lost Travel Documents (SLTD) database.[117]

The API evaluation report briefly mentioned that with the introduction of the ESP, via which API data could be matched against multiple databases, the potential for countering terrorist threats may grow.[118] However, no further remarks are made in that respect. Furthermore, the report finds that API data will play a central role in interoperability, as implemented by the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). In particular, Member States currently receive API data in a batch format exchanged directly between the airline and the Member State. However, upon establishing the EES and the consequent abolition of stamping, carriers will no longer be able to know whether a visa was used or not by a third-country national. In that respect, a 'carrier gateway' will be set up and carriers will have to consult the EES to verify whether third-country

[110] Ibid, art 20.

[111] Interoperability Regulations, arts 6-11.

[112] Ibid arts 12-16.

[113] Ibid arts 17-24.

[114] Ibid arts 25-36.

[115] Ibid art 39.

[116] HLEG, 'Final report' (2017).

[117] Commission, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205 final.

[118] Commission, 'Study on Advance Passenger Information (API) (n 6) 75.

nationals holding a Schengen visa for one or two entries will have already used the number of entries authorised by their visa. Similarly, when the ETIAS becomes operational, carriers will similarly have to verify the status, including the validity of an ETIAS travel authorisation.[119] The aforementioned developments will require several changes at a technical level on how API data is collected and the industry-recommended technology for facilitating this is an interactive API (iAPI), so that API data will be sent once through a single point (the carrier gateway) to different destinations, both centralised systems and national systems.[120] It must be noted that these considerations are in line with the conclusions of the HLEG that has stressed that in the future, interactive API data will be necessary to enable carriers to check a travel authorisation and to check remaining authorised stay.[121] The HLEG further pointed out that Member States could opt, on a voluntary basis, for a single router or hub (an API hub), perhaps hosted by eu-LISA, that could collect such data from carriers and transfer them to the relevant central and national entities.[122]

[119] For both systems, such checks will be carried out through the introduction of the Interactive Query. See EES Regulation, art 13; ETIAS Regulation, art 45.

[120] Commission, 'Study on Advance Passenger Information (API) (n 6) 61.

[121] HLEG, 'Final report' (n 116) 39.

[122] Ibid.

3. OVERVIEW OF THE API PROPOSALS

The previous section demonstrated that the API legal framework is not fit-for-purpose in numerous respects; it is a very broad and loose framework, which had led to wide discrepancies at national level, whereby air carriers are subject to different requirements and personal data processed in very different ways. Besides, API data are transferred from through old fashioned means, such as fax machines. To bring the API-related data up to speed the Commission adopted two proposals, one in connection with the collection and transfer of API data for enhancing and facilitating the effectiveness and efficiency of border checks at external borders and of combating irregular immigration and a separate one on the processing of API data for law enforcement purposes. This section will concisely explain the main features of each proposal.

3.1. The API border management proposal

The API border management proposal is based on Article 77(2)(b) (measures relating to the checks to which persons crossing external borders are subject) and (d) (establishment of an integrated management of external borders) and 79(2)(c) TFEU (measures on 'illegal immigration and unauthorised residence, including removal and repatriation of persons residing without authorisation'). It constitutes a development on the Schengen *acquis* regarding external borders and to which Ireland participates.[123] As a result, the API border management Regulation would apply to Bulgaria, Cyprus and Romania, even though the controls at their internal borders have not yet been lifted.

3.1.1. Scope

The API border management proposal only covers air carriers conducting scheduled or non-scheduled flights into the EU.[124] According to Article 3(c), flights into the EU means 'flights flying from the territory either of a third country or of a Member State not participating in this Regulation, and planned to land in the territory of a Member State participating in this Regulation'. Therefore, no API data will be collected from flights originating in Bulgaria, Cyprus and Romania into the Schengen area and vice versa, although border checks still exist at internal air borders between these countries and the other Member States. The application to flights **into the EU** as opposed to flights **into the Schengen area** is important; an approach whereby API data would be collected on all flights into the Schengen area would automatically mean that flights from Ireland, as a non-Schengen state, Bulgaria, Cyprus and Romania, as Member States where the controls at their internal borders have not been lifted, would fall within the scope of API-related obligations.[125]

In turn, outbound flights are not covered by this proposal; border authorities would only receive the API data after the physical exit checks of the travellers and examinations of the travel documents, therefore too late to support their work. As explained in the Explanatory Memorandum attached to the proposal, the full API data set is generated once the passengers are on board a plane, therefore the border guards would only receive the API data after the physical exit checks of the travellers and the examination of their passports, which would be too late to support the work of the border guards.[126]

[123] Therefore, flights from Ireland into the Schengen area and *vice versa* are not covered by the scope of the proposal.

[124] Commission, 'API border management proposal' (n 15) art 2.

[125] See Council, Document 7770/23 (23 March 2023).

[126] Commission, 'API border management proposal' (n 15) 8-9.

Furthermore, the API border control proposal does not envisage the collection and transfer of API data from other means of transport, such as maritime, rail and bus transport operators. With regard to sea carriers, this is because, as explained in the previous section there already exist EU and international rules requiring maritime transport operators to transfer passenger information in advance to Member States' border authorities for incoming and outgoing routes. Therefore, duplication of requirements would not meet the necessity test. As for land carriers the collection of API data is particularly challenging due to the lack of advance check-in processes and the lack of systematic issuance of nominative tickets. Therefore, any extension of the obligations to land transport would require heavy investments in the physical infrastructure of operators, with substantial consequences on their economic model and on passengers.

3.1.2. Categories of API data collected by air carriers

According to Article 4, air carriers must collect API data of travellers, consisting of the traveller data and the flight information. Traveller data involve:

(a) the surname (family name), first name or names (given names);

(b) the date of birth, sex and nationality;

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

(d) the date of expiry of the validity of the travel document;

(e) whether the traveller is a passenger or a crew member (traveller's status);

(f) the number identifying a passenger name record used by an air carrier to locate a passenger within its information system (PNR record locator);

(g) the seating information, such as the number of the seat in the aircraft assigned to a passenger, where the air carrier collects such information; and

(h) baggage information, such as number of checked bags, where the air carrier collects such information.

As for the flight information, this concerns the following elements:

(a) the flight identification number or, if no such number exists, other clear and suitable means to identify the flight;

(b) when applicable, the border crossing point of entry into the territory of the Member State;

(c) the code of the airport of entry into the territory of the Member State;

(d) the initial point of embarkation;

(e) the local date and estimated time of departure;

(f) the local date and estimated time of arrival.

3.1.3. Processing of API data for border management purposes

The **collection** of API data by air carriers must take place in a way that ensures that API data are accurate, complete and up-to-date.[127] To that end, collection of certain API data (name, date of birth,

[127] Ibid art 5(1).

sex and nationality, type and number of the travel document and the three-letter code of the issuing country of the travel document and the date of expiry of the validity of the travel document) will be done using automated means from the machine readable data of the travel document of the traveller concerned.[128] The automated means must be reliable, secure and up-to-date[129] and have been preferred to modernise the process entailing manually transcribed information as has been the case to date. If the use of automated means is not possible due to the travel document not containing machine-readable data, air carriers must collect that data manually, in a manner ensuring accuracy, completeness and the up-to-date character of the data. The Commission is empowered to adopt delegated acts with regard to the technical requirements and operational rules, to which air carriers will be subject. [130]

The data will no longer be transferred to the national authorities, but to a router by electronic means pursuant to detailed rules that will be adopted by the Commission in delegated acts on the common protocols and supported data formats.[131] The **transfer to the router** must take place at the moment of check-in and immediately after flight closure, once passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or to leave the aircraft.[132] In cases where an air carrier becomes aware, after having transferred data to the router, that the API data are inaccurate, incomplete, no longer up-to-date or were processed unlawfully, or that the data do not constitute API data, it must immediately inform eu-LISA. The latter must immediately inform the competent border authority that received the API data transmitted through the router.[133]

The **retention period** of the API data is 48 hours (from 24 hours in the API Directive) both for the air carriers and the competent border authorities from the moment of departure of the flight, after which period they must be immediately and permanently deleted.[134] However, where an air carrier or competent border authority becomes aware that the data collected, transferred or received are inaccurate, incomplete, no longer up-to-date or were processed unlawfully, or that the data do not constitute API data, it must immediately either correct, complete or update, or permanently delete, that API data.[135]

3.1.4. Router

A novelty of the revision of the API legal framework is the establishment of a router that will be designed, developed, hosted and technically managed by eu-LISA,[136] for the purpose of facilitating the transfer of API data by the air carriers to the competent border authorities and to the PIUs (as per the API law enforcement proposal).[137] It is proposed that the router will be used exclusively by air carriers to transfer API data and by competent border authorities and PIUs to receive API data.[138] Its technical architecture will comprise (a) a central infrastructure, including a set of technical components enabling

[128] Ibid art 5(2).

[129] Ibid art 5(3).

[130] Ibid art 5(4).

[131] Ibid art 6(1) and (3).

[132] Ibid art 6(2).

[133] Ibid art 6(4).

[134] Ibid art 8(1) – (2).

[135] This is without prejudice to the possibility for air carriers to retain and use the data where necessary for the normal course of their business in compliance with the applicable law.

[136] Commission, 'API border management proposal' (n 15) arts 22-24.

[137] Ibid art 9(1).

[138] Ibid art 10.

the transmission of API data; (b) a secure communication channel between the central infrastructure and the competent border authorities and the PIUs, and a secure communication channel between the central infrastructure and the air carriers.[139] Furthermore, according to Article 9(3), to the extent technically possible, it will share and re-use the technical components of the EES web service,[140] the ETIAS carrier gateway[141] and the VIS carrier gateway.[142]

The router will immediately and in an automated manner transmit the API data to the competent border authorities of the Member State where the flight will land[143] in accordance with technical rules laid down in Commission delegated acts[144] These must be designated at the national level and be included in a publicly available list compiled by the Commission.[145] Only authorised staff of the competent border authorities must have access to the API data.[146]

API data must be stored on the router only insofar as necessary to complete the transmission to the relevant competent border authorities (or the PIUs in relation to the law enforcement use of API data) and must be deleted from the router, immediately, permanently and in an automated manner in both of the following situations: (a) where the transmission of the API data to the relevant competent border authorities and PIUs has been completed; in respect of the API law enforcement proposal, where the API data relates to other intra-EU flights than those for which the requirement to transfer the data exists.

To ensure security and integrity of API data, logs of data processing operations must be kept by eu-LISA.[147] According to Article 12, the logs must cover the following: (a) the air carrier that transferred the API data to the router; (b) the competent border authorities and PIUs to which the API data were transmitted through the router; (c) the date and time of the transfers and place of transfer; (d) any access by staff of eu-LISA necessary for the maintenance of the router; (e) any other information relating to those processing operations necessary to monitor the security and integrity of the API data and the lawfulness of those processing operations. Air carriers are also obliged to create logs of all processing operations and will cover the date, time, and place of transfer of the API data.[148] The logs must be protected against unauthorised access and other security risks [149]and must be kept for one year starting from their creation, after which period they must be deleted immediately and permanently. However, if the logs are needed for procedures for monitoring or ensuring the security and integrity of the API data or the lawfulness of the processing operations and these procedures have begun at the moment

[139] Ibid art 9(2).

[140] EES Regulation, art 13.

[141] ETIAS Regulation, art 45.

[142] VIS Regulation, art 45c.

[143] Commission, 'API border management proposal' (n 15) art 11(1). According to Article 20, Member States must ensure that border authorities are connected to the router so that they can receive, further process and exchange in a lawful, secure, effective and swift manner.

[144] A dedicated and updated table of correspondence between the different airport of origin and destination and the countries to which they belong will be kept by eu-LISA. Ibid art 11(1).

[145] Ibid art 11(2) and (4).

[146] Ibid art 11(3).

[147] Ibid art 13(1) and (3). The logs will not contain personal data other than those to identify the relevant eu-LISA staff member.

[148] Ibid art 13(2). According to Article 14(4) eu-LISA and air carriers must ensure that the logs are protected from unauthorised access and other security risks.

[149] Ibid art 13(4).

of the expiry of the time period then the logs must be kept for as long as necessary for those procedures.[150]

Moreover, the API border management proposal contain rules on what action must be taken when it is technically impossible to use the router either due to its own failure or because the systems or infrastructure have failed at the national level or of an air carrier.[151] In addition, liability regarding the router in case of damage is with the Member State or the air carrier, unless and insofar as eu-LISA failed to prevent the damage.[152] The router is meant to start operations by means of an implementing act once eu-LISA is ready.[153] In the meantime, air carriers may use the router in implementation of the rules under the API Directive following an agreement with the receiving authority.[154]

3.1.5. Data protection provisions

According to Article 15, the competent border authorities will be controllers in relation to the processing of API data constituting personal data through the router, including the transmission and the storage for technical reasons of that data in the router, as well as in relation to the processing of API data received by the air carriers. Furthermore, the air carriers will also be considered as data controllers for the processing of API data constituting personal data in relation to their collection and transfer of that data. In turn, eu-LISA will be considered as processor for the processing of API data through the router.[155]

The API border management proposal also foresees rules on the security of API data, which must be ensured by all three entities[156] and must cooperate with each other to that end.[157] Furthermore, according to Article 18, air carriers and border authorities are subject to self-monitoring of their compliance with their API-related obligations, including through frequent verification of the logs.

With regard to supervision, Article 19 provides that national data protection authorities must conduct audits on the processing operations of API data by the competent border authorities in accordance with the relevant auditing standards, at least once every four years.[158] Similarly, the EDPS must ensure an audit of processing operations of API data performed by eu-LISA at least once every year. A report on that audit must be sent to the European Parliament, the Council, the Commission, the Member States and eu-LISA, which will have an opportunity to make comments before its adoption.[159] Upon request, eu-LISA must supply information requested by the EDPS, who must be granted access to all documents it requests and to the logs, as well as access to the premises.[160]

Article 29 (under Chapter 6) further provides that Member States must designate one or more national supervisory authorities responsible for monitoring the application of the API-related rules and ensure compliance. Member States must ensure that the national supervisory authorities have all the

[150] Ibid art 13(5).

[151] In the case of air carriers, they must submit to the competent supervisory authority a report containing all necessary details on the technical impossibility, including its reasons, its extent, consequences and measures taken to address it.

[152] Commission, 'API border management proposal' (n 15) art 26.

[153] Ibid art 27.

[154] Ibid art 28.

[155] Ibid art 16.

[156] For eu-LISA's responsibilities see Article 17(2).

[157] Ibid art 17.

[158] Ibid art 19(1).

[159] Ibid art 19(2).

[160] Ibid art 19(3).

necessary investigative and enforcement powers to carry out their tasks, including by imposing penalties. Furthermore, they must lay down detailed rules on the performance of those tasks and the exercise of those powers, ensuring that the performance and exercise is effective, proportionate, and dissuasive and is subject to safeguards in compliance with the fundamental rights guaranteed under EU law.

With regard to penalties, the API border management proposal differs from the API Directive. In particular, there are no minimum or maximum penalties prescribed, but rather they must be effective, proportionate and dissuasive.[161]

Finally, a practical handbook, in the form of a recommendation, must be devised by the Commission, in close cooperation with the PIUs, other relevant Member States' authorities, the air carriers and relevant EU agencies, which shall be made publicly available, containing guidelines, recommendations and best practices for the implementation of the rules.[162]

3.1.6. The first steps towards the integration of API data into the interoperability framework

Finally, API are progressively integrated into the interoperability framework. In addition to the use of architectural components from the EES, ETIAS and VIS, a novelty of the revised framework concerns the compilation of statistical data. The data will concern the functioning of the router, compiled on a quarterly basis, showing in particular the number, nationality and country of departure of travellers, specifically those who boarded aircrafts with inaccurate, incomplete or no longer up-to-date API data, with a non-recognised travel document, without a valid visa, without a valid travel authorisation or reported as overstay, as well as the number and nationality of travellers.[163] The statistics will be stored at one of the interoperability components: the CRRS. Furthermore, eu-LISA shall compile statistical data in an annual report to be transmitted to the European Parliament, the Council, the Commission, the EDPS, the European Border and Coast Guard Agency and the national supervisory authorities.[164] At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects.[165]

eu-LISA will have the right to access the following API data solely for the purposes of the reporting and for generating statistics, without however such access allowing for the identification of the travellers concerned:

(a) whether the traveller is passenger or a crew member;

(b) the nationality, sex and year of birth of the traveller;

(c) the date and initial point of embarkation, and the date and airport of entry into the territory of a Member State arrival;

(d) the type of the travel document and the three letter code of the issuing country and the date of expiry of the travel document;

(e) the number of travellers checked-in on the same flight;

(f) whether the flight is a scheduled or a non-scheduled flight;

[161] Ibid art 30.

[162] Ibid art 32.

[163] Ibid art 31(1).

[164] Ibid art 31(3).

[165] Ibid art 31(4).

(g) whether the personal data of the traveller is accurate, complete and up-to-date.

To enable the compilation of statistical data through the CRRS, Article 35 of the proposal foresees changes to the Interoperability Regulation for border checks and visas that the CRRS will support the objectives of the API Regulation.

3.2. The API law enforcement proposal

The adoption of a separate proposal for the use of API data for law enforcement purposes is legally appropriate, given the different purposes for which API data are processed and the fact the processing of API data is a development on the Schengen *acquis*. The API law enforcement proposal is based on Articles 82(1)(d) and 87(2)(a) TFEU. A number of provisions are common with the API border management proposal.

The proposed rules complement the provisions of the PNR Directive by imposing specific obligations on air carriers to collect API data in specific situations and to transfer those data in a specific manner. To the extent that the proposed rules correspond and overlap with those of the PNR Directive, the latter prevails as *lex specialis* and *lex posterior*. Besides, the definition of PNR data in the PNR Directive includes any API data collected. The Regulation would merely provide the rules on the collection and transfer of API data from the air carriers through the router to the PIUs and do not regulate further processing of such data, which will be subject to the PNR Directive, as well as subject to the limits and safeguards established therein and by the CJEU in *Ligue des droits humains*. The rules of subsequent processing of API data by the PIUs, such as on the specific purposes of the processing, retention periods, deletion, exchange of information, transfer by the Member States to third countries and provisions on the protection of personal data, are those set out in the PNR Directive, as interpreted by the CJEU in *Ligue des droits Humains*,

3.2.1. Scope

The API law enforcement proposal concerns collection, transfer to the router and transmission to the PIUs of API data **on extra-EU flights and selected intra-EU flights**, both scheduled and non-scheduled.[166] As a result, the scope of obligations goes beyond the prescriptions of the first proposal, which only concerns extra-EU flights. According to Recital 8, the PNR Directive does not cover domestic flights, that are flights that depart and land on the territory of the same Member State without any stop-over in the territory of another Member or a third country, and they are not covered by the proposed rules either. This is without prejudice to the possibility for Member States to provide, under their national law and in compliance with EU law, for obligations on air carrier to collect and transfer API data on such domestic flights.

3.2.2. Processing of API data for law enforcement purposes

The rules of the API border management are largely replicated here as well. Therefore, API data must be collected (some of which through automated means) and transferred to the router.[167] An additional provision involves code-shared flights: where the flight is code-shared the obligation to transfer the API data will be on the air carrier that operates the flight.[168] There is also an obligation for air carriers to

[166] Commission, 'API law enforcement proposal' (n 17) art 2.

[167] Ibid art 4.

[168] Ibid art 4(1).

immediately either correct, complete or update or permanently delete the API in any of the following situations:

- when they become aware that the API data collected are inaccurate, incomplete or no longer up-to-date or were processed unlawfully,

- or that the data transferred do not constitute API data; where the transfer of the `API data has been completed.[169]

In both cases, eu-LISA must be informed, which must in turn inform the relevant PIUs that received the information.

Once the data have been transmitted to the router, the latter must immediately and in an automated manner transmit them to the PIU of the Member State on the territory of which the flight will land, or from the territory of which the flight will depart or to both in case of intra-EU flights.[170] PIUs must thus be connected to the router.[171] Where there are stop-overs to other Member States, then the data must be transmitted to the PIUs of all the Member States concerned.[172] Where it is technically impossible to use the router, the API law enforcement proposal envisages rules mirroring those of the API border management proposal.[173]

As regards which intra-EU flights will fall within the scope of the proposed rules, if Member States wish to make use of this possibility, Article 5(2) foresees that where Member States must each establish a list of the intra-EU flights concerned and shall provide to eu-LISA by the date of application of the Regulation. Those Member States must regularly review and where necessary update those lists and immediately provide the Agency with any such updated lists. The information contained on those lists must be treated confidentially.

Article 6 foresees obligations for keeping logs by air carriers, covering the date, time and place of transfer of API data, that should be kept for one year unless needed for monitoring or ensuring security and integrity of API data or the lawfulness of the processing operations and the procedures have started before the one year deadline.

3.2.3. Data protection and other rules

Both the PIUs and the air carriers shall be data controllers.[174] No rule on the role of eu-LISA is foreseen. Security of the API data must also be ensured by the PIUs and air carriers, which must further cooperate with each other and with eu-LISA to ensure such security. [175] The rules on self-monitoring, liability, supervision, penalties and the practical handbook are identical or almost identical to adapt to the distinction between border authorities and PIUs.[176]

[169] Ibid art 4(8).

[170] Ibid art 5.

[171] Ibid art 10.

[172] Ibid.

[173] Ibid art 13.

[174] Ibid art 7.

[175] Ibid art 8.

[176] Ibid arts 9 and 14-17.

As with the API border management proposal, changes to the Interoperability Regulation for police and judicial cooperation, asylum, and migration to reflect the compilation of statistical data via the CRRS.[177]

[177] Ibid art 18.

4. LEGAL ASSESSMENT OF THE PROPOSALS

The assessment of the proposals reforming the API legal framework will primarily concern the fundamental rights implications of the proposed rules as enshrined in the Charter and interpreted by the CJEU and the European Court on Human Rights (ECtHR), with special focus on the rights to respect for private life (Article 7 of the Charter and Article 8 of the European Convention on Human Rights – ECHR), protection of personal data (Article 8 of the Charter), freedom of movement (Article 45 of the Charter) and to conduct business (Article 16 of the Charter).

4.1. Horizontal clause on fundamental rights

At the outset, it must be noted that Recital 6 of both API proposals refer to fundamental rights stating that:

> 'The collection and transfer of API data affects the privacy of individuals and entails the processing of personal data. In order to fully respect fundamental rights, in particular the right of respect for private life and the right to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union ('Charter'), adequate limits and safeguards should be provided for.'

Whereas this is welcome provision, as noted by the FRA officials, there is no fundamental rights safeguard which would be horizontally applicable. Such a provision, which can be found in similar border management and law enforcement instruments, for example in Article 14 of the ETIAS Regulation, would be necessary to be included in the operative part of the text. Furthermore, the API proposals refer solely to the rights to privacy and data protection, but reference to the principle of non-discrimination (Article 21 of the Charter), as discriminatory treatment of air travellers based on API data (or on statistical data fed into reports by eu-LISA, as it will be explained below), and the right to an effective remedy (Article 47 of the Charter).

4.2. Interference of the API framework with fundamental rights

The API data to be processed by the proposed rules include, inter alia, besides the name(s) of the air passenger(s), information relating to the flight, information concerning baggage and seating. In line with Opinion 1/15 and *Ligue des Droits Humains,* since the API data include information on identified individuals, namely air travellers, the various forms of processing to which those data may be subject affect the fundamental right to respect for private life.[178] Furthermore, the processing of API data falls within the scope of the right to protection of personal data, because the API-related obligations entail processing of personal data and, therefore, must necessarily satisfy the data protection requirements laid down in that article.[179]

In particular, the communication of personal data to a third party, such as a public authority, constitutes an interference with the rights to privacy and protection of personal data, irrespective of the subsequent use of the data at national level. Retention of personal data and access to those data with a view to their use by public authorities also constitute interferences. The sensitivity of personal data or whether the persons concerned have been inconvenienced in any way are irrelevant for finding an interference.[180] In the case of the API system, the transfer of API data from air carriers, which are separate

[178] By analogy to *Ligue de droits humains* (n 18) para 95.

[179] Ibid para 96; See Opinion 1/15 (n 80) para 123.

[180] Ibid para 96; Opinion 1/15 (n 80) paras 124 and 126. See *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

data processing activities, in this case to the router managed by eu-LISA as well as the transmission from the router to border authorities and the PIUs constitute interferences with the rights guaranteed in Articles 7 and 8 of the Charter.

To assess the **seriousness of the interference** with the rights the following factors must be taken into account:

1. The API proposals entail the systematic and continuous transfer to border authorities of API relating to any air passenger on incoming extra-EU flights from third countries and in the case of law enforcement on incoming and outgoing extra-EU flights and selected intra-EU flights. Therefore, there are some limitations in terms of the scope of the obligations in terms of delimiting the means of transport to air carriers and in respect of specific types of flights.

2. API data is only a subset of PNR data and therefore, taken as a whole, the data may reveal a complete travel itinerary, but not other information regarding travel habits, relationships existing between one or more persons and the financial situation of air passengers, their dietary habits or state of health, or other sensitive information.[181]As the EDPS has noted, the processing is less compared to the processing of PNR data.[182]

3. The API data transferred by air carriers are intended to assist in border management and fighting irregular migration and in the context of law enforcement, for advance assessment, prior to the passengers' scheduled arrival or departure, as well as subsequent assessment.[183] However, the API proposals do not lay down the rules on the subsequent assessments, which must take place pursuant to the Schengen Borders Code and the PNR Directive respectively.

In addition, to the extent that API law enforcement proposal entails the processing of selected intra-EU flights, it interferes with the freedom of movement as guaranteed by Article 3(2) TEU and Article 45 of the EU Charter.

Finally, the right of air carriers to conduct business is also impacted given that the API framework entails obligations to collect and transfer API data through specific means, additional categories of personal data and with specific obligations regarding their retention.

4.3. Justification for the interferences resulting from the API proposals

The aforementioned fundamental rights are not absolute, but must be considered in relation to their function in society.[184] According to Article 52 of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made to those rights and freedoms, only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In that regard, Article 8(2) of the Charter states that personal data must, inter alia, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

[181] By analogy to *Ligue des droits humains*, (n 18) para 100.

[182] EDPS, 'Opinion 6/2023 on the Proposals for Regulations on the collection and transfer of advance passenger information (API)' (2023) 6.

[183] By analogy to *Ligue des droits humains* (n 18) para 101.

[184] Opinion 1/15 (n 80) para 136.

The principle of legality is observed; the API data are listed, and the API proposals provide a framework for the collection, transfer, and transmission through detailed rules. The essence of the rights is also not compromised; by analogy to *Ligue des droits humains*, the nature of the API information is limited to certain aspects of a person's private life concerning air travel and does not provide a full overview of their private life – in fact, compared to PNR data a narrower aspect of a person's air travel is revealed, no sensitive data are processed, the purposes for which the data must be processed are laid down and the proposals contain rules on the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing.[185]

Both proposals pursue objectives of general interest to the EU: in relation to the API border management proposal, the management of external borders has been a longstanding policy aim of the EU since the abolition of internal border controls. As for the API law enforcement proposal, the findings in *Ligue des droits humains* are directly applicable in this case. The purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes undoubtedly constitute objectives of general interest of the EU that are capable of justifying even serious interferences with the fundamental rights to privacy and data protection.[186]

The appropriateness of the API system is also not called into question; in line with international standards, the processing of API data in advance through checks at the national level constitutes a mechanism that can assist in speeding border controls for air travellers and drawing the attention of border authorities to individuals who may require further attention.

In light of the above, the next sub-sections focus on a proportionality test to assess the extent to which the proposed rules go beyond what is necessary and proportional in light of the aims pursued. The sub-sections examine the scope of the API proposals, including efforts to expand the proposed scope, the offences for which API data may be processed, the categories of personal data processed, the nature of the router, the role of eu-LISA under data protection law, the retention period of API data, the (lack of reference to) individual rights and supervision.

4.3.1. Scope of the API proposals

The API proposals concern only the collection, transfer and transmission of API data to border authorities and the PIUs. The processing of API data after transmission to the PIUs is subject to the PNR Directive and the national laws transposing that Directive. This relationship between the API law enforcement Regulation and the PNR Directive should be made clear in the legislation either in the Preamble or in Article 1 regarding the scope of the proposed rules.

In terms of which modes of transport are covered, the API proposals are limited to air carriers. The API border management proposal concerns only flights into the EU, whereas the API law enforcement proposal refers to extra-EU flights, both outgoing and incoming, and intra-EU flights, which is further specified to concern flights selected by the Member States.

a. Processing of API data on both incoming and outgoing extra-EU flights as well as selected intra-EU flights for border management purposes

With regard to the obligation of transferring API data for border management purposes, the preferred approach is in line with the right to free movement, as processing API data of intra-EU flights would amount to checking travel documents for border control purposes and thus a reintroduction of internal

[185] *Ligue des droits humains* (n 18) para 120.

[186] Ibid para 122.

border controls. As mentioned in *Ligue des droits humains*, such an obligation 'would amount to allowing the competent authorities, when internal borders of the said Member State are crossed, to ensure systematically that those passengers can be authorised to enter its territory or to leave it and would thus have an effect equivalent to the checks carried out at external borders with third countries'.[187]

Furthermore, as mentioned in Section 3, outbound flights are not covered because they would be received too late to support the work of border authorities. Besides other mechanisms such as the reinforcement of checks against relevant databases at external borders in accordance with the Schengen Borders Code[188] and the forthcoming use of the EES are sufficient to achieve the same results, and therefore an expansion of the scope of the API border management proposal would not meet the necessity test.

That said, there have been calls to expand the mandate to outgoing extra-EU flights arguing that this would be aligned with the API law enforcement proposal and the ICAO Annex 9, which defines the API system as an electronic communication system whereby required data elements are collected and transmitted to border control agencies 'prior to flight departure or arrival' and made available on the primary line at the airport of entry.[189] Furthermore, Annex 9 states that API involves the capture of a passenger's or crew member's biographic data and flight details by the aircraft operator prior to departure, which is electronically transmitted 'to the border control agencies in the destination or departure country'. These arguments are weak. First, because the alignment with API law enforcement proposal cannot be achieved, as intra-EU flights would not be covered and in any case, necessity should be determined based on actual operational needs. The second argument is also not convincing because the ICAO does not mandate transmission to the authorities of both the destination or departure.

b. Processing of API data on both incoming and outgoing intra-EU flights for law enforcement purposes

One of the main novelties of the API law enforcement proposal is that it extends the obligation for the transfer of API data to intra-EU flights. In addressing the concerns expressed by the CJEU in *Ligue des droits humains* regarding the proportionality of processing PNR data of passengers on intra-EU flights, the proposal includes specific limitations. The selected flights will be those under Article 2(3) of the PNR Directive, which enables the extension of PNR requirements to only select intra-EU flights, as interpreted by the CJEU. API data will only be processed for intra-EU flights selected by the Member States. The selected flights must be set out on a confidential list communicated to eu-LISA, which will be regularly updated.[190]

Furthermore, Article 12(b) of the API border management proposal foresees the deletion from the router of any intra-EU flight API data other than those in the list 'immediately, permanently and in an automated manner'. Similarly, air carriers would be obliged to permanently and immediately delete API from intra-EU flights after the completion of the transfer to the router.[191] The proposed technical

[187] Ibid para 290.

[188] Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L74/1.

[189] Belgium already has this obligation for air carriers to transmitted API data for border management purposes when passengers intend to leave the EU or have already left the EU. See Law 25.12.2016, Article 29§2.2.

[190] Commission, 'API border management proposal' (n 15) art 5 and recital 14.

[191] Commission, 'API law enforcement proposal' (n 17) art 4(8)(b).

solution, namely the use of the router, will limit the transmission of API data to PIUs in selected flights only and will ensure that the information of which intra-EU flights have been selected will remain confidential in order not to jeopardise internal security.[192]

From the outset, the analysis on the selection of intra-EU flights and the transmission of API data to the PIUs in connection to those flights are intertwined with questions about the nature and function of the router and the role of eu-LISA in this context. Therefore, this analysis is relevant for Sections 4.3.4 and 4.7 below.

The selection of the intra-EU flights must take place in line with the requirements of *Ligue des droits humains*. In particular, first the Court has stressed that 'the Member States' power to extend the application of the system […] to intra-EU flights is to be exercised in full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter'.[193] Second, the CJEU has further clarified that when a Member State wishes to exercise the power either for all intra-EU flights or only for such selected flights, is not exempt from the requirement to verify that the extension selected or all intra-EU flights is effectively necessary and proportionate for the purposes of attaining the objective of the PNR Directive.[194] Third, in a situation where the Member State establishes that there are sufficiently solid grounds for considering that it is confronted with a 'genuine and present or foreseeable' terrorist threat the application of the PNR system to all intra-EU flights from or to that Member State, for a limited period of time, does not go beyond what is strictly necessary.[195] In the absence of such a terrorist threat, the application of the directive cannot be extended to all intra-EU flights, but must be limited to intra-EU flights relating, inter alia, to certain routes or travel patterns or to certain airports for which there are, at the discretion of the Member State concerned, indications that would justify that application. The decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists.[196] The strictly necessary nature of that application to the selected intra-EU flights must be regularly reviewed in accordance with changes in the circumstances that justified their selection.[197] Moreover, the Court found that the collection of PNR data linked to cross-border travel within the EU could infringe on freedom of movement, as enshrined in Article 45 of the Charter and constitute an impermissible restriction to that freedom.[198]

Against this backdrop, it must be assessed whether the proposed rules would lead to the *en masse,* indiscriminate and systematic transmission of all intra-EU API data to PIUs beyond the standards required by the CJEU and whether the proposed solution with the existing safeguards is proportionate to the aims pursued. A key issue in this respect is the fact that the API law enforcement proposal refers to the judgment in Recital 14. Whereas that recital provides a brief account of the CJEU's findings it may be worth adding to it the main components of the findings in more detail to provide clarity. This is all the more necessary considering that there is no forthcoming revision of the PNR Directive.

[192] Ibid 11.

[193] *Ligue des droits humains* (n 18) para 167.

[194] Ibid para 168.

[195] Ibid para 171.

[196] Ibid para 172.

[197] Ibid paras 173-74.

[198] Ibid paras 278-279.

The EDPS Opinion argues that the prior filtering of API data by the router on the basis of the list submitted by the Member States and regularly updated and the immediately and automated deletion of all data outside the lists by both the air carriers and the router could preclude the possibility for PIUs to receive and process in any manner API data from intra-EU flights that they are not allowed to.[199] At the heart of this assessment is the understanding that the collection and transfer of the API data to the router and the subsequent transmission to the PIUs for processing are data processing operations which are intertwined.[200] According to the EDPS, there appears to be no less intrusive means with comparable guarantees and safeguards for intra-EU flights. This solution would not technically or legally allow PIUs to have access to API data from flights not formally selected and communicated to eu-LISA. In an informal discussion with Officials from the EDPS it was further explained that in this assessment emphasis is placed on the ultimate aim of the judgment is to prevent the systematic processing of all intra-EU API data by the PIUs.

This study will provide additional considerations on the compatibility of the transmission of the API data to the router of all intra-EU flights with the requirements of *Ligue des droits humains*. According to the CJEU:

> 'the application of the system established by the PNR Directive to selected intra-EU flights must be limited to the *transfer and processing* of the PNR data of flights relating, inter alia, to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application.'[201]

Therefore, the mere transfer of API data by air carriers to the router for selection in itself and on its own constitutes an interference with the rights to respect for private life and protection of personal data irrespective of their further storage (in the router), selection and transmission to the PIUs in accordance with the lists provided by the Member States. This interpretation is supported by longstanding and settled case law of the European courts, which distinguish the interferences with the rights under Articles 7 and 8. In particular, as highlighted earlier in Section 4, in accordance with *Weber and Saravia v Germany*[202] and more recently confirmed in Opinion 1/15[203] and *Ligue des droits humains*, communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated.

In light of the above, the use of the router as a channel for the transfer of all intra-EU flights seems problematic in terms of compliance with *Ligue des droits humains*, because it entails the blanket collection and transfer of API data in connection to all intra-EU flights, which are filtered, thus processed, at a second stage through the router. It will also not be in line with the principle of data minimisation enshrined in Article 5(1)(c) of the GDPR, according to which the personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Whether there is no other elegant solution from a technical perspective that on the one hand, would not jeopardise internal security – by essentially requiring Member States to disclose to air carriers how they select which intra-EU flight data are of interest, and on the other hand, would not allow the blanket transfer of API data directly to the PIUs, as is the current (and unlawful) practice

[199] EDPS (n 182) 7.

[200] Ibid 8.

[201] *Ligue des droits humains* (n 18) 174. Emphasis added.

[202] *Weber and Saravia v Germany* (n 180).

[203] Opinion 1/15 (n 80) para 124.

requires further discussion. In particular, considering that the router was not part of the Impact Assessment of the reform of the API framework, it is unclear whether an alternative technical solution, which could entail the filtering of the API data already at the stage of the transfer by air carriers, without the need of a middleman was feasible, with the addition of any safeguards to prevent air carriers (some sort of pull method, with encryption key). In view of the importance of the CJEU's pronouncements on this matter and the clear limitations provided arguably the revision of the API framework could have been postponed until another Impact Assessment, this time solely focusing on this matter, was imperative.

That said, despite the router being viewed by the EDPS as the best solution given the circumstances, it must be ensured that the selection process is subject to a series of requirements in line with *Ligue des droits humains*. This is not sufficiently achieved in the API law enforcement proposal and there is room for improvement. In particular, as highlighted by the Meijers Committee, the proposal allows significant discretion to select intra-EU flights and to subsequently amend this selection without the inclusion of any criteria for the assessment made by Member States for the selection of intra-EU flights.[204] Therefore, it may be worth exploring the inclusion of a clear assessment criteria for the collection and transfer of API data of intra-EU flights. Member States may not be negative towards this inclusion, which will bring clarity to the rules, but it must be ensured that the criteria are sufficiently specific. Furthermore, the confidential nature of the list may prevent the foreseeability of the processing of personal data and effective oversight to ensure the strict necessity of this measure. This will not be in line with *Ligue des droits humains* where it was held that the decision providing for application to intra-EU flights must be open to effective review, either by a court or by an independent administrative body. In other words, this confidentiality creates opacity and to prevent this, it must be ensured that an independent administrative, parliamentary, and/or judicial oversight mechanism exists. This suggestion is also in line with *Big Brother Watch v United Kingdom*, which concerned a different, yet related surveillance regime on retention of telecommunication data and the European Court of Human Rights (ECtHR) found that the use of selectors (filters) was subject to the Convention requirements of necessity and proportionality, as well as internal and external oversight.[205] Such oversight cannot be conducted by eu-LISA; such functions are not supported by the mandate of this agency, which can only operate as a technical agency which provides technical support in implementing the filters of the Member States. eu-LISA must promptly respond to changes in the list with the selected intra-EU flights. Such a requirement for swift implementation of any revisions to the list can be inserted in Article 5(2) of the API law enforcement proposal.

Notwithstanding the fact that the router as a selector of intra-EU flights on behalf of Member States, there is increasing desire by Member States to favour another solution whereby air carriers would directly transfer API data from all intra-EU flights to PIUs, which will then select from which flights they will process API data.[206] This approach mirrors the current practice at national level that entails *en masse*, indiscriminate and systematic surveillance through the processing of API data of all intra-EU flights, beyond those selected. The process of selecting and deleting API data at the national level constitutes processing of personal data and therefore is in direct contravention of *Ligue des droits humains*. It also entails risks of abuse by Member States, which may simply continue business as usual disregarding the findings of the CJEU. Admittedly, PIUs have a very distinct way of functioning and may

[204] Meijers Committee, 'Comment on the Legislative Proposals Providing for Collection and Transfer of Advance Passenger Information (API) (March 2023).

[205] *Big Brother Watch v UK,* Appl nos 58170/13, 62322/14 and 24969/15 (Judgment of the Grand Chamber of 25 May 2021) para 421.

[206] Council, Document 7651/1/23 (13 April 2023).

be set in specific ways, whereby all data are subject to automated analysis, but these practices remain incompatible with EU law.

c. Extension of API-related obligations to other modes of transport

One of the main points of disagreement is whether the scope of the API system could be further extended to other modes of transport due to the growing number of travellers by train in Europe and operational needs.[207] Recital 35 of the API border management proposal provides for this possibility, but there are not further requirements in the proposals. Although it appears that this matter has settled for now and the API proposals will go ahead with their scope solely on air carriers, there are discussions on possible extension in the future to sea and land carriers. Therefore, for the purpose of providing a holistic approach, this study will merely include certain important considerations. To our understanding, the Commission has been invited to conduct feasibility studies in this respect in the future.

First, it must be observed that the collection of API data by land carriers would interfere with the rights to privacy and the protection of personal data, and therefore should only be possible under strict conditions and following a thorough assessment of its necessity and proportionality. Furthermore, to the extent that any such obligations would extend to intra-EU transports, they will restrict the freedom of movement of EU citizens, which, is only permitted for the purpose of combating terrorism and fighting organised crime, and under strict conditions. For the purpose of facilitating border and migration control, it would amount to a reintroduction of internal border controls in contravention of EU law.[208]

With regard to sea carriers, an extension of API obligations could be easier to achieve, considering that, as stressed in Section 2, there are extensive obligations for ships and ferries, whereby the categories of data collected from sea passengers mirror those under the API border management proposal. According to Council Document 7082/23, three options are under consideration, all of which would entail the transfer of data by sea carriers based on the existing FAL forms, as the established format and by making use of the European Maritime Single Window environment. These options are: the extension of reporting obligations to ferry connections with ports situated in third countries, which are exempted from the Schengen Borders Code.[209] However, in view of the fact the recent adoption of Regulation (EU) 2019/1239, it remains unclear why there is insistence on revising the existing framework. A second option would extend the obligation to outbound and inbound maritime transport for law enforcement purposes. This would require a clear case on necessity and proportionality and must be in line with the requirements of *Ligue des droits humains*. This involves the third option, which is highly intrusive and involves the possibility of intra-EU maritime travel for law enforcement purposes. As FRA officials have stressed, it is doubtful that such an extension would be in line with the spirit of the judgment, which is clearly oriented towards strictly delimiting surveillance of mobility. Besides, extending the scope of the API law enforcement proposal would not be sufficient, as there are no rules on the processing of API data from maritime operators by PIUs.

With regard to land carriers, as Table 2 shows (and mentioned in Section 2) very few Member States have extended API obligations in this respect. With regard to PNR data, in some Member States PNR data are already collected for other modes of transport other than air traffic. In particular, according to the 2020 Commission report on the implementation of the PNR Directive, Belgium extends the

[207] Council, Document 6230/23 (13 February 2023).

[208] Meijers Committee (n 204) 6.

[209] Schengen Borders Code, Annex VI, 3.2.9(i).

collection of PNR data to international high-speed trains and the international bus sector, although that implementation is at early stages. Estonia collects ferry passengers' data. French legislation foresees the collection of API and PNR data for maritime transport. In Sweden, the police and customs authority have access to passengers' data from other modes of transport, but the scope of the applicable legislation is more limited than the PNR Directive.[210] These national approaches make the case for extending the scope of API obligations quite thin; if Member States have not set up such systems at national level, it is unclear which operational needs exist. In view of the specific characteristics in terms of infrastructure, passenger journey and density of networks it is unlikely that such extension would even be feasible. A key challenge is that in some countries it is popular to purchase tickets that are not tied to a specific person and a specific connection. Such forms of distribution would have to be banned in the future or companies would be obliged to collect API data before departure. Technical equipment would have to be purchased and installed to check all passenger at boarding and disembarking, which would require substantial financial investment. An additional challenge consists of the existence of intermediate stops where passengers can embark or disembark, sharing of platforms between different types of trains, high number of passenger stations of travel etc.[211] Overall, an extension to bus and rail carriers would have drastic impact on their business models of land carriers and passengers. Therefore, significant changes in the way bus and rail carriers operate would be expected, making these modes of transport less attractive. This will also constitute an interference with the right to conduct business, enshrined in Article 16 of the EU Charter.

Table 1: Processing of API data in other modes of transport

Other modes of transport	Member States
Sea carriers	Austria, Belgium, Estonia, Spain, France, Hungary, Malta, Norway, Finland and Iceland
Railway	Estonia, France, Finland
Bus	Austria

Source: Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (2020) 43.

d. Non-scheduled flights

Article 2 of the API border management proposal refers to scheduled and non-scheduled flights; the former term involves flights that operate according to a fixed timetable, for which tickets can be purchased by the general public; the latter term concerns flights that do not operate based on a fixed timetable and that it is not necessarily part of a regular or scheduled route. The scope of non-scheduled flights is somewhat unclear and it is not clarified in the Preamble. For example, military or medical flights seem to fall within the term, but there may be reasons of national security that may prevent the

[210] Commission, Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SWD(2020) 128 final.

[211] Council, Document 6853/1/23 (2 March 2023) 5.

disclosure of information about the passengers. Therefore, the meaning of non-scheduled flights should be clarified.

e. Transiting passengers

With regard to air passengers in transit from a third country, who arrive in the EU from a third country and directly continue onwards a flight outside the EU, there is no reference to this within the API proposals. For example, a Turkish national flying from Istanbul to Mexico City via Amsterdam. Transit (or connecting) flights enable passengers to reach their final destination through two or more flights, after a brief stop-over at the airport. One single ticket is issued, and the passenger does not change planes or airlines. In such cases, the advance passenger data is sent by the air carrier to the final destination country that will effectively perform the entry border check of passengers. Therefore, in such cases, no API data will be delivered to the Netherlands in the scenario outlined above concerning the Turkish national. The passenger would not enter the Schengen area and would not undergo an entry check at the external borders.[212] The API Regulations must contain a clear provision that transit flights are not included within the scope.

4.3.2. Offences for which API data may be processed

Article 1 of the API law enforcement proposal refers to the subject matter of the legal instrument which involves the collection, transfer and transmission of API data from air carriers for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes. Article 3(l) and (m) of the proposal defines terrorist offences and serious crimes by reference to the PNR Directive. In particular, 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 in Framework Decision,[213] now replaced by Directive 2017/541,[214] in Articles 3 to 12. 'Serious crime' refers to the offences listed in Annex II of the PNR Directive that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.

In *Ligue des droits humains*, the CJEU clarified the scope of these offences noting these offences should be interpreted as defined in the relevant area of national and/or EU law.[215] Furthermore, the application of the PNR system must be effectively limited to combating serious crime and that the system does not extend to offences that amount to ordinary crime.[216] Importantly, application of the system must be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.[217] Considering the close link between the API law enforcement proposal and PNR Directive, it is of added value to incorporate these findings of the judgment in the legislation, at least in a recital to bring clarity and uniform application.[218] They would place Member States under specific obligations to bring the legislation in line with the judgment.

[212] Commission, 'Commission Staff Working Document – Impact Assessment' (n 44) 25.

[213] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism [2002] OJ L164/3.

[214] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
[2017] OJ L88/6.

[215] *Ligue des droits humains* (n 18) para 147.

[216] Ibid para 152.

[217] Ibid paras 153-157.

[218] This argument has been reiterated by the FRA officials.

4.3.3. Categories of API data processed

Article 4(2) and (3) API border management proposal expands the categories of personal data collected compared to those prescribed in the API Directive. These data fields are also to be transmitted to PIUs in accordance with Article 4 of the API law enforcement proposal. Recital 8 refers to the list as 'clearly and exhaustively' laying down the categories of API data processed. Article 4 includes a closed and mandatory list could be reflected also in the text.

Table 2: Categories of personal data

Categories of personal data	API Directive	API border management proposal	Council compromise proposal[219]
Traveller data	Number and type of travel document used	Type and number of travel document used and **three-letter code of the issuing country**	Type and number of travel document used and three-letter code of the issuing country
	Nationality	Nationality	Nationality
	Full names	Surname (family name), first name or names (given name)	Surname (family name), first name or names (given name)
	Date of birth	Date of birth	Date of birth
Flight information	Border crossing point of entry into the territory of the Member States	Border crossing point of entry into the territory of the Member State	Border crossing point of entry into the territory of the Member State
	Code of transport	Code of the airport	Code of the airport(s)
	Departure and arrival time of the transportation	**Local date and time of departure and of arrival**	Local date and time of departure and of arrival
	Total number of passengers carried on that transport	-	
	Initial point of embarkation	Initial point of embarkation	Code of airport of the initial point of embarkation

[219] Council, Document 7753/23 (24 March 2023) 7-8.

Additional personal and flight information		Date of expiry of validity of the travel document	Date of expiry of validity of the travel document
		Sex	Sex
		Whether the traveller is crew or passenger	Whether the traveller is crew or passenger
		PNR locator record	PNR locator record
		Seating information, such as the number of the seat	Seating information
		Baggage information, such as the number of checked bags	Baggage information, such as the weight and the number of checked bags
		Flight identification number	Flight identification number
			Code indicating the method used to capture and validate data
			Code of airport of departure of the flight
			Contact information of the air carrier
			Format used for data transfer

Source: Authors' compilation

A closed and mandatory list of API data that would be collected is imperative because it will bring legal certainty, standardisation and uniformity in the requirements at national level. In accordance with *Ligue* *des droits humains* it must meet the requirements of clarity and precision.[220] Furthermore, it is important to clarify that the primary purpose of processing API data is border management and therefore processing API data for law enforcement purposes should be considered as an ancillary, secondary purpose. Consequently, the necessity and proportionality of the personal data processed must be determined in light of the primary purpose, rather than the secondary one. In that regard, it is welcomed that the API proposals only provide one list of API data in Article 4 of the API border management proposal. Furthermore, the list should be in line with the ICAO API Guidelines.

Compared to the currently applicable API Directive, the proposed rules entail a significant increase in the categories of personal data to be transmitted to national authorities through the router. In particular, the sex, the three-letter code of the issuing country of the travel document, and elements (d) to (h) on the traveller data are all new additions. Furthermore, with regard to the flight information, the flight identification number is a new addition; at the same time, the proposed rules do not require the transmission of the total number of passengers carried on that transport, as was mandated in Article 3(2) of the API Directive.

First, with regard to the date of expiry of the validity of the travel document, the sex of the traveller and the three-letter code of the issuing country, this information is contained in the MRZ of a travel document and their addition would align with ICAO's PAXLST standards.[221] Because they can be found in the MRZ, their collection would be primarily automated. Besides, already most Member States request the collection of the data in the MRZ for border control purposes (in fact in several Member States this practice dates back to the implementation of the API Directive in 2006).[222] Therefore, in this respect the addition would merely modernise the legislation to be in line with national laws.

Second, the majority of Member States already collect information on the scheduled departure and arrival time, therefore that information would also align to current practices and with the WCO/ICAO standards.[223] Scheduled flight departure and arrival data would complete current departure and arrival times. This also constitutes an alignment with international standards and would reconcile the planned versus actual departure and arrival times[224] allowing for more accurate information processed.

Third, information about the traveller's status, whether the data relates to a crew member, or a passenger is less clear. The Commission Impact Assessment summarily refers to the findings of the Study supporting the Impact Assessment.[225] With regard to the distinction between crew and passenger data, that Study referred to the international standards according to which Member States have the option to request API crew data, which are already collected by air carriers. Crews are exempt from the requirements of the forthcoming EES and ETIAS[226] and in accordance with Article 20(1)(b) and Annex II of the Schengen Borders Code they are subject to specific rules regarding border checks, which therefore necessitate a specific justification as to why crew members who are subject to pre-vetting requirements in the form of security checks should also be subject to the API legal framework. Evidence about the necessity of this distinction is missing.

[220] *Ligue des droits humains* (n 18) paras 126-140.

[221] Commission, 'Study supporting an impact assessment' (n 96) 31.

[222] Ibid 29.

[223] Ibid 29-30.

[224] Ibid 32.

[225] Commission, 'Commission Staff Working Document – Impact Assessment' (n 44) 79.

[226] ETIAS Regulation, art 2(2)(i); EES Regulation, art 2(3)(g).

Fourth, on the information regarding seating and baggage, this is an area that merits further attention because this information may potentially reveal some additional aspects of a person's private life. The wording of certain data fields for collection could be clarified; in particular, with regard to the seat number and baggage the use of the phrase 'such as' is not exhaustive and does not provide clarity as to what other information in relation to the seat number and the baggages could be collected. For the baggages for example, it is unclear whether API data would include information about the fragility or whether it was to be reclaimed on priority. For the seat number it is unclear what other information, aside from the seat number, could be collected and further processed.

Fifth, the passenger record locator number will support the joint processing of API and PNR data and therefore that information would be useful.

The last point to be clarified is the following: when it comes to which API data must be collected and transferred to the router, the API law enforcement proposal refers to the data fields in Article 4(2) and (3). At the same time, heading 18 of Annex I of the PNR Directive that lays down which categories of PNR data air carriers are required to provide to the PIU refers to 'any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)'. In *Ligue des droits humains*, the CJEU has clarified that 'the information to which it refers is exhaustively the API data listed in the said heading as well as in Article 3(2) of the API Directive'.[227] A revision of the API data fields would therefore signify that the phrase 'any advance passenger information (API) data collected' includes exhaustively the categories of personal data that Article 4 of the API border management proposal.

4.3.4. The router

This analysis on the router must be read in conjunction with the previous considerations under Section 4.3.1 regarding its function as filtering which intra-EU flights are selected by the Member States so that the router would transmit only the API data relating to those flights to the PIUs. These considerations are complemented by a broader examination in Section 4.7 of the router as an information exchange channel aiming to remedy the decentralised nature of the API and PNR systems and as a step towards the integration of API data in the interoperable framework.

For this section, the aim is to critically assess the nature of the router and the surrounding safeguards for its proportionate functioning as the 'mailman' and the 'middleman' between the air carriers and the national authorities. The first issue to clarify is the nature of the router. As mentioned by FRA officials, it would appear that the idea of the router has emerged as a mechanism to address the findings of the CJEU in *Ligue des droits humains*. Indeed, the Study supporting the Impact Assessment that was published in 2021 did not mention (and thus did not consider the necessity and proportionality of) the development of a router. The Impact Assessment refers to the router as a way that would 'substantially reduce the transmission costs for air carriers' – because API data would be transmitted to a single point.[228] It also highlighted that the router would accommodate a general ICAO recommendation (SARP) for a single-window API transmission.[229] However, as this was not in the plans previously and

[227] *Ligue des droits humains* (n 18) 138.

[228] Commission, 'Commission Staff Working Document – Impact Assessment' (n 44) 30.

[229] Ibid 84.

was not subject to a prior assessment, it appears that the use of the router for the selection of flights has been a central reason why the router was introduced.[230]

A router is a device that is designed to take data packets to the appropriate parts of a computer network. A similar router has been proposed in the context of the Prüm proposal as well.[231] As evidenced from the wording used in the API proposals, a series of the router's functions mirror those of a database, though as an EDPS official mentioned it is closer to the functions of a cable. The conclusion that some functions of the router are similar to those of database is drawn based on certain qualities of the router: it has the capacity to even for a very short period of time store the API and it enables access by eu-LISA in accordance with Article 23(3) of the API border management proposal, when this is strictly necessary for the maintenance of the router and for drawing statistical data on a daily basis to compile reports. These conflicting functions of the router blur a clear understanding of its nature. They also beg the question whether the use of the router in this context may lead to a function creep whereby the router will be used for purposes other than those for which they have been originally foreseen, a point that is explored below in Section 4.7. Understanding and correctly labelling the functions and the nature of the router as a database is important because it determines which data protection safeguards must be in place for its lawful functioning. In particular, as the EDPS has noted and FRA officials have agreed, the need for effective safeguards ensuring a high level of security are particularly important and should be present in both legal instruments.[232] Whereas Article 17 of the API border management proposal is in the right direction in this respect, the respective provision in the API law enforcement proposal seems to be underdeveloped.[233] In particular, pseudonymisation and encryption in the transmission of the API data to the national authorities from the router should be implemented to the extent possible.

Another consideration is the extent to which the API data on the different types of flights should be stored altogether in the router or whether they should be kept in silos considering that some of these data (on outgoing extra-EU and intra-EU flights) are only to be used in the context of law enforcement. This suggestion could flow from *Ligue des droits humains* by analogy. The CJEU found that:

> 'Member States cannot create a single database containing both the PNR data collected under the PNR Directive and relating to extra-EU and intra-EU flights and the data of passengers of other means of transport as well as the data covered by Article 3(2) of the API Directive, in particular where that database can be consulted not only for the purposes referred to in Article 1(2) of the PNR Directive but for other purposes also.'[234]

Furthermore, the extent to which the router should have additional automated functions checking the quality and completeness of the data[235] in the same way that eu-LISA checks the quality of personal data in large-scale IT systems (e.g. that the format of the data is in compliance with the set standards) is also to be discussed. In view of the fact that the non-legislative acts will provide specifications and binding requirements for the messaging format, the router could measure compliance with those standards. Such functionality of the router is not included in the API proposals and given that one of

[230] This came from an observation by a FRA official.

[231] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' COM(2021) 784final.

[232] EDPS (n 182) 8-9.

[233] Commission, 'API law enforcement proposal' (n 17) art 8.

[234] *Ligue des droits humains* (n 18) para 289.

[235] Council, Document 7651/1/23 (n 206) 23.

the main stakes of the revision is to improve the quality of the API data, as evidenced by the emphasis on their collection through automated means from the MRZ of the travel document, it may be worth exploring such suggestion. As in the case of information systems, where eu-LISA is a data processor, a data quality check should not affect the responsibility of the agency as a data processor and it will not signify that the agency will have access to the API data.

The last aspect that requires attention is the co-existence of the router with the requirements of the PNR Directive that states that PIUs are responsible for the collection of PNR data from the air carriers and that Member States must ensure that air carriers transmit PNR data to the database of the PIU.[236] Does this mean that in the absence of a revision of the PNR Directive, air carriers would have to transfer the API data to the router, which will then forward them (following any necessary selection) to the PIUs, whereas the PIUs will continue to receive the rest of the PNR data from the air carriers? This is a particularly confusing matter that undermines the effectiveness of the router. One way to bypass the limitations of the PNR Directive is to rely on Article 16(4) of the eu-LISA Regulation, according to which a group of at least five Member States may entrust the Agency with the task of developing, managing or hosting a common IT component to assist them in implementing technical aspects of obligations deriving from EU law on decentralised systems in the Area of Freedom, Security and Justice. Those common IT solutions shall be without prejudice to the obligations of the requesting Member States under the applicable Union law, in particular with regard to the architecture of those systems. However, this relies on the initiative of Member States and does not provide legal certainty or clarity on the matter.

4.3.5. The role of eu-LISA

The development of the router managed by eu-LISA brings to the fore important questions regarding the attribution of roles and responsibilities to the agency. Article 16 of the API border management proposal assigns to eu-LISA the role of a data processor in relation to API data constituting personal data. The extent to which this division of roles is in line with the data protection framework, taking into account the Guidelines by the EDPS Guidelines on the concepts of controller, processor and joint controllership under the EU General Data Protection Regulation (EU DPR), as well as the Guidelines by the European Dara Protection Board (EDPB) on the concepts of controllers and processor in the GDPR, requires particular attention, as different arguments have been proposed by the EDPS and by Member States.

On the one hand, according to the EDPS, the Member States acting as controllers determine the purposes and essential means of the processing via the router. The term 'essential means' are closely linked to the purpose and the scope of the processing. Concerning the purposes, although eu-LISA will process all API data, through storage in the router, transmission to the competent border authorities and PIUs and access to API data to compile statistical data, the data eventually processed at national level are those in relation to flights selected by the Member States. It is therefore the Member States that determine which specific subsets of data they receive and for which purposes. Furthermore, concerning the essential means these are determined by the law, which lays down the scope of the API rules, the categories of personal data, the retention period, and which authorities have access.[237] The non-essential means relate to more practical aspects, such as the hardware or software that will be used and can be determined by the processor. eu-LISA will merely provide the communication channel between the air carriers and the national authorities, which is not a database, though it does have some

[236] PNR Directive, arts 4(1) and 8(1).

[237] EDPS (n 182) 10.

temporary storage functionalities, and will not have other purposes for processing the API data except for transmitting them to national competent authorities. In light of the above, the EDPS has concluded that eu-LISA is correctly designated as data processor.

On the other hand, Member States have expressed their preference to designate eu-LISA as a data controller, 'as the responsibilities of eu-LISA as a processor could not fully support border authorities in the entirety of their responsibilities' and the agency would behave in a way similar to controllers.[238] Another argument is that the router is an infrastructure the concrete design of which fall entirely within eu-LISA's area of responsibility and national border authorities will have no influence.[239] Processing on behalf of a controller presupposes that the data controller has the possibility to influence the processor, which it has been argued that this is not the case with the API framework. It has been proposed that Article 17 which concerns the responsibility of eu-LISA with regard to the security of API data it processes are obligations that would otherwise affect data controllers, therefore, eu-LISA is actually a controller.[240]

Arguably, this is a 'schizophrenic' approach by Member States, which on the one hand, do not wish for eu-LISA to grow too much and on the other hand, they may wish to use the agency as a means to get away from their responsibilities for processing API data.[241]

Recognising that this is a grey area, this study will offer additional considerations ultimately opting for the approach of the EDPS for several reasons. First, the approach of eu-LISA as a processor has been opted in the case of the revision of the Prüm framework, which also foresees the use of a router.[242] Second, from a pragmatic standpoint assigning the role of a controller to eu-LISA could create fragmentation and diffusion on responsibility and complication as to which actor is ultimately responsible for the processing of API data. Any storage of the data until they will be transmitted to the Member States they must be deleted and the storage period is particularly short. Thus, this storage is very limited and only to the extent that it serves the purpose of feeding the API data to the Member States. Third, assigning eu-LISA with the role of a controller is incompatible with previous approaches, whereby calls of the EDPS to clearly assign responsibility to eu-LISA as a controller have failed. In general, eu-LISA has been designated as either a processor, such as in the case of interoperability,[243] or data controller in relation to data security, as in the case of ETIAS.[244] However, it does not make any sense as a concept and it would rather further confuse matters and diffuse responsibility than provide clarity and the attribution would be too complex from the perspective of individual rights. In other words, if eu-LISA would be designated as a data controller, an overhaul of the legal bases of all large-scale IT systems managed by eu-LISA should take place in order to determine whether the delineation of responsibilities has been correctly assigned by law. In any case, whether the law has correctly assigned a role to eu-LISA could be subject to a future evaluation to determine whether the legal framework corresponds to what happens in practice.

[238] Council, Document 7651/1/23 (n 206) 13.

[239] Council, Documents 7327/1/23 (23 March 2023) 4; 7651/1/23 (n 206) 29.

[240] 7327/1/23 4.

[241] Discussion with FRA officials (24 April 2023).

[242] Commission, 'Prüm II proposal' (n 231) art 53.

[243] Interoperability Regulation for border checks, art 41.

[244] ETIAS Regulation, art 57.

4.3.6. Retention period of API data

The retention period of API data is doubled – from 24 hours to 48 hours. This increase in the retention period is not explained in the Explanatory Memorandum or the Impact Assessment. The 2020 Evaluation Study on API found that when processing API data for border control purposes, the majority of Member States store API data for 24 hours.[245] Some Member States as well as all Schengen associated countries allow national authorities to store the data collected for longer than 24 hours.[246] However, the Study does not specify how long that retention period is. The Study supporting the Impact Assessment was not concerned with the retention period of the data either. The same applies to air carriers, whereby eight Member States as well as all Schengen associated countries allow national authorities to store the data collected for longer than 24 hours and only Austria provides a 48-hour retention period of API data by air carriers.[247] In light of the above, the extension of the retention period is without justification and therefore is problematic.

4.3.7. Individual rights

Travellers whose personal data are transferred to the router and from there to competent border authorities and PIUs are entitled to a series of individual rights in accordance with data protection law, namely the rights to access, rectification, erasure and restriction and rights to compensation and judicial redress. Such rights are laid down in Article 13 of the PNR Directive, which refers to Framework Decision 2008/977/JHA,[248] now replaced by the LED. However, in the case of the API proposals there is no reference to individual rights. This is surprising considering that the API Directive, despite its laconic wording, did contain at least a right of information.[249] It is true that these proposals constitute sectoral data protection legislation laying down specific rules in the context of the collection and transfer of API data, therefore the provisions of the GDPR and the LED are respectively applicable; the former in connection to the collection of API data by air carriers and the processing by border authorities; the latter in respect of the processing of API data by PIUs. The EU Data Protection Regulation is also applicable with respect to any processing of personal data by eu-LISA (through its router or for the development of statistical data). In any case, a clear delineation of individual rights and their application of the generally applicable legislative instruments on the protection of personal data is missing from both proposals.

4.3.8. Supervision

One confusing matter in the API border management proposal is the inclusion of provisions relating to supervision in two different chapters. Articles 19 and 29 both refer to supervision. A separate provision on supervision of eu-LISA by the EDPS, referring also to the audits stated in Article 19. Despite the increased role of eu-LISA in the operationalisation of the revised API framework in relation to the router, the proposals do not lay down a provision regarding the supervision of the agency by the EDPS (except the references in Article 19 on the audit of processing operations by eu-LISA). Therefore, the role of the EDPS in supervising eu-LISA – irrespective of whether under the rules the agency is data controller or

[245] See Commission, 'Study supporting an impact assessment' (n 96).

[246] Austria, Czech Republic, France, Hungary, Ireland, Italy, Lithuania, Poland, United Kingdom. Ibid.

[247] Ibid 34.

[248] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

[249] API Directive, art 6(2).

data processor – could also be mentioned by adding a provision regarding the supervision of the agency and cross-referring to EUDPR.

Furthermore, an equivalent provision on the conduct of audits by PIUs similar to Article 19 of the API border management proposal does not exist in the API law enforcement proposal. Article 15 of the PNR Directive on the supervision by national DPAs states that these entities must verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint. Therefore, the specific time frame that is prescribed in the API border management (an audit at least once every four years) is not foreseen and leaves leeway regarding the frequency of audits.[250]

In addition, Article 29 of the API border management proposal and Article 15 of the API law enforcement proposal contain rules on supervision of the implementation of API-related obligations at the national level by air carriers. These provisions are almost identical – the sole differences concern the applicable general data protection legal instruments – and both refer to supervision by national supervisory authorities. The provisions, however, are somewhat unclear, particularly Article 29(2) and 15(2) which refers to the Member States' obligation to ensure 'that the performance and exercise [of the national supervisory authorities' tasks and powers] is effective, proportionate and dissuasive and is subject to safeguards in compliance with the fundamental rights guaranteed under Union law'. This phrase is unusual for provisions regarding the supervision of data processing activities and reflects provisions regarding the imposition of penalties. A clearer understanding of the scope of these provisions is necessary.

One last matter that is a general concern regarding the API framework more broadly refers to the increasingly occurring issue stemming from the symbiotic relationship between different actors (public bodies, private carriers and EU agencies), with divergent mandates, such as border and law enforcement authorities, which apply different data protection frameworks (GDPR, LED and the EU Data Protection Regulation). The ability of national DPAs to ensure data protection relies not only on sufficient human, financial and technical resources to adequately fulfil their supervisory tasks but also on the coordination between national DPAs and the EDPS. Therefore, coordinated supervision may play a significant role in enabling effective supervision.

4.4. Penalties

Article 30 of the API border management proposal and Article 16 of the API law enforcement proposal do not prescribe a range of minimum and maximum sanctions unlike the API Directive. This leaves ample room for discretion for Member States, which seems to have been preferred in order to accommodate the divergent practices at national level. According to the evaluation of the API Directive, different amounts are applicable for carriers which have failed to collect and correctly transmit API and the range of pecuniary fines is extensive, ranging from 100 euros in Germany to 500,000 euros in Ireland.[251] In practice, 17 Member States have not imposed any sanctions to carriers and solve any defects through cooperation and coordination between airlines and national authorities.[252] In 14 countries, fines have been imposed for the violation of obligations related to the transmission of API data, with great variations between the number of sanctions and the annual

[250] Meijers Committee (n 204) 3.

[251] Commission, 'Study on Advance Passenger Information (API)' (n 7) 48-49.

[252] Ibid.

average of fines in euros.[253] Eight Member States have made use of the possibility of imposing additional sanctions, such as immobilisation, seizure and confiscation of assets, but none of them imposed in practice other sanctions, besides pecuniary penalties, yet.

It is true that this difference in approach may cause uncertainty and confusion to air carriers and therefore different types of infringement attached to a range of sanctions being specified in the legislation may be an alternative approach.[254] This approach could increase uniformity at the national level, but may not be feasible. It is also not in line with Article 14 of the PNR Directive, which also gives flexibility to Member States.

4.5. The compilation of statistical data

Article 31 of the API border management proposal foresees that eu-LISA will store the daily statistics in the CRRS that will involve the number, nationality, country of departure of the travellers, and specifically of the travellers who boarded the aircraft with inaccurate, incomplete or no longer up-to-date API data, with a non-recognised travel document, without a valid visa, without a valid travel authorisation, or reported as overstay, the number and nationality of travellers. There are several issues arising from the compilation of such statistical data.

First, it is unclear how eu-LISA will provide such statistics based on API data solely, when the API will not involve information regarding the visa or the ETIAS authorisation or the status of a traveller as an overstay. The provision indicates that the statistical data will be developed using data from information, namely VIS, EES and ETIAS and the data will be combined to draw conclusions on travellers.

Second, Article 31(5) explicitly states that eu-LISA will have the right of access to specific API data – excluding the name of travellers, but including many other categories of personal data. As mentioned above, the personal data processed by eu-LISA raise data protection concerns regarding the role of the agency as a data controller, data security[255] and the need for supervision by the EDPS. They raise additional concerns as to whether the lack of access to the name of a traveller and the travel document number are sufficient for not allowing identification, though there is no explicit reference to anonymisation. This is interesting, considering that Article 39(3) of the Interoperability regulations stresses the anonymity of the data stored in the CRRS. Furthermore, it is unclear whether indirect identification through the combination of different data elements may take place. For example, as FRA had mentioned in its Opinion on the Interoperability Regulations, in case of individuals from small island states in the Pacific, even where the name and the passport number are removed, an individual may still be identified through a combination of nationality, sex and year of birth.[256]

Third, as also highlighted by FRA officials, the way in which statistical data will be used may raise fundamental rights concerns. Statistical data may be used for risk analysis, profiling or predictive risk assessment, which may be to the detriment of specific groups of travellers. Concerns about the potential use of statistical data are all the more pertinent considering that according to Article 41(4), the Commission may request eu-LISA to provide it with statistics on specific aspects related to the

[253] In Austria, for instance, over the last eight years, around 1,000 sanctions have been imposed, with an annual average of 651,260 euros. Similarly, in Germany, more than 1,400 cases have been issued with annual fines ranging from 407,882 euros (in 2012) to 2,905,090 euros (in 2018).

[254] Council, Document 5805/3/23 (21 March 2023) 3.

[255] See EDPS (n 182) 11.

[256] FRA, 'Interoperability and fundamental rights implications' (2018) 43.

implementation of the API rules. In this context, the reports may consciously or unconsciously incorporate subconscious bias suggesting operational actions which would result in discrimination of certain categories of persons,[257] for example by using the statistical data to feed into automated and non-automated risk assessments of travellers, for example by the PIUs. As noted by the Meijers Committee, 'if eu-LISA's statistics suggest that travellers of specific nationalities or with travel documents issued by specific countries are involved with illegal immigration more often than other travellers, then competent border authorities could select travellers of these nationalities or with these travel documents for extra controls after a risk assessment'.[258] The statistical data could thus result in discriminatory border control, whereby some travellers from specific nationalities or point of embarkation may be subject to increased and repeated checks.

4.6. Practical handbooks

Both proposals foresee the publication of practical handbooks drafted by the Commission in close cooperation with the national competent authorities – border authorities or PIUs – the air carriers and relevant EU agencies. The practical handbooks will be released in the form of a recommendation and must be made publicly available. The provisions, Article 32 and 17 respectively, are welcome, however it may be useful to further specify which other national authorities could be involved in this process as well as which agencies. eu-LISA is such an agency, but other than that it is unclear which other agencies should have a role in this respect. Presumably this will concern the EBCG Agency, as involved in the EU border management. Other agencies that may have a constructive role in identifying and promoting good practices in line with the protection of fundamental rights are the EDPS and the FRA.

4.7. The router as the enabler of interoperability

The creation of the router should thus not be viewed independently, but must be considered in conjunction with the forthcoming interoperable framework. According to the Explanatory Memorandum attached to the proposals, the need for EU action on API data to some extent stems from recent legislative developments on Schengen external border management, namely the establishment of two large-scale IT systems for third-country nationals, the EES and the ETIAS.[259]

The interaction between the API framework and large-scale IT systems takes place in two main respects; they re-use the technical components from the EES, ETIAS and VIS for the transfer of API data to the router and importantly, that API data will feed into the statistics stored in CRRS, which is one of the interoperability components. Though officially no further interaction is proposed, the Explanatory Memorandum of the API border management proposal explains that:

> 'Establishing a centralised transmission mechanism for API data at EU level is a logical continuation of this concept. Following the concepts included in the Interoperability Regulations, the centralised transmission of API data could in the future lead to using this data to query various databases (SIS, Europol data) via the European Search Portal.'[260]

The aforementioned remark points to the direction that the development of the router is not merely a way of a technical channel to deliver the data from the air carriers to the competent border authorities and PIUs. Rather the introduction of the router is a way of **rectifying the decentralised approach in**

[257] Ibid 43-44.

[258] Meijers Committee (n 204) 5-6.

[259] Commission, 'API border management proposal' (n 15) 5.

[260] Ibid.

the processing of API data, by bringing them all together through storage in the router, so that border control authorities will be able to search and consult them alongside data from databases in the ESP. It is speculated that the next steps would then be for PIUs to have access to the CIR for law enforcement purposes. This is merely speculated but the documentation available clearly hints towards the further development of the interoperability framework. **The router would thus have a much more important function in the future of border management and law enforcement, but the full picture is not clear just yet.** The end goal of developing interoperability should feed into the assessment of the necessity and proportionality of the router; whereas the router as a technical channel for data exchange may seem as a relatively limited technical change in the way in which air travellers data are transferred to the Member States, in reality it will be **the motor through which the different structures - centralised and decentralised systems - will be reconciled and integrated**. However, **viewing the router from a technical perspective and limited to functioning as 'the mailman' for the API data, may mask broader fundamental rights consequences**.[261] A 'salami', step-by-step approach whereby seemingly minor changes are introduced, but a much more comprehensive plan is underway is well known in the development of large-scale IT systems, hence this dystopian picture is more than simply rhetoric. The creation of the router is the first, decisive step towards the integration of API in the interoperability framework; once the router is developed and operational, it is easier for Member States and EU institutions to call for amendments to the legislation in order to harvest the potential of major financial investment and get the most out of the new tool.

4.8. Delegated acts

Though the proposals are primarily assessed from the perspective of fundamental rights, there are is an additional issue that requires examination relating to the adoption of non-legislative acts to supplement the legal framework. The API legal framework requires to be supplemented by a number of delegated acts in accordance with Article 290 TFEU, as follows:

1. Article 5(4) (API border management) and Article 4(5) (API law enforcement): to lay down detailed technical requirements and operational rules for the collection of API data using automated means;

2. Article 6(3) (API border management) and Article 5(3) (API law enforcement): to lay down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of API data to the router;

3. Article 20(2) (API border management) and 10(2) (API law enforcement): to lay down the necessary detailed rules on the connections to and integration with the router for the competent border authorities and PIUs respectively;

4. Article 21(2) (API border management) and 11(2) (API law enforcement): to lay down the necessary detailed rules on the connections to and integration with the router for the air carriers.

Recitals 31 (API border management) and 24 (API law enforcement) provide in this respect that

> '[i]t is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of

[261] For similar arguments see Valsamis, Mitsilegas, 'Interoperability as a Rule of Law Challenge' (Migration Policy Centre) https://migrationpolicycentre.eu/interoperability-as-a-rule-of-law-challenge/ accessed 27 April 2023.

> delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts'.

The extent to which the use of delegated acts is appropriate is debatable. According to the Interinstitutional Agreement on Non-binding Criteria for the application of Articles 290 and 291 TFEU of 18 June 2019 measures establishing a procedure to ensure the uniform implementation of a rule laid down in a legal instrument should be adopted by means of an implementing act. Member States have expressed their preference to implementing acts, which provide higher control by the Member States in the process. This is due to the fact that implementing acts are formally voted on by Member States, whereas delegated acts are not. Therefore, with implementing acts the Member States will have possibilities to influence these issues.[262] The Commission has replied that these acts should be prepared in an inclusive manner, because the issues concern only Member States' competent authorities, and do not involve carriers. Presuming the impact on data formats used by carriers it is even more important to have a workable system.[263]

That said, an implementing act has been adopted in the case of the PNR Directive, with regard to Article 16(3), which concerns the adoption of rules on common protocols and supported data formats in the case of transfers of PNR data to air carriers.[264] Similarly, in the context of interoperability, the rules on developing the Universal Message Format (UMF) standard are laid down in a Commission Implementing Decision.[265] Therefore, there is merit in the Member States' argument that non-legislative acts should be implementing acts rather than delegated acts.

[262] Council, Document 7651/1/23 (n 206) 23.

[263] Council, Document 6853/1/23 (n 211) 1.

[264] Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units [2017] OJ L113/48.

[265] This is a secret document. It is known due to the EDPS comments on Commission Implementing Decisions on laying down and developing the Universal Message Format (UMF) standard pursuant to Article 38(3) of Regulations (EU) 2019/817 and 2019/818 of the European Parliament and of the Council.

5. CONCLUDING REMARKS AND POLICY RECOMMENDATIONS

This study aimed to provide background information on the Commission's proposals to reform the API framework and to provide a legal analysis on their implications primarily with respect to fundamental rights. As it has been demonstrated, the revision of the API regime is timely, considering that the API Directive was adopted in 2004 and the framework provided therein has been not only loose leading to significant divergences in national implementation but also outdated due to various developments at international and EU level.

The CJEU judgment in *Ligue des droits humains* is landmark and any revision to the API regime must be in line with the Court's pronouncements in full, without creating loopholes and loose interpretations. This is all the more pertinent considering that there is no information available regarding the revision of the PNR Directive to bring its content in line with the significant restrictions provided by the CJEU.

Against this backdrop, the study wishes to provide the following policy recommendations which can be drawn from the analysis in Section 4:

- Introduction of a horizontal provision in the operative part of the proposals with regard to the protection of fundamental rights, which will refer to all relevant fundamental rights in question, including the right to an effective remedy (under Article 47 of the Charter) and the principle of non-discrimination.

- Inclusion in Recital 14 or elsewhere in the API law enforcement Regulation of a clear, concise and full outline of the CJEU requirements, as laid down in particularly with regard to intra-EU flights.

- The scope of the API border management proposal is limited to what is necessary and proportionate. No further extension of the obligations in relation to incoming flights should be foreseen.

- The scope of the API law enforcement proposal extends to both outgoing and incoming extra-EU flights as well as selected intra-EU flights. The selection of these flights would take place through a router, developed and managed by eu-LISA. From a legal perspective, the development of the router is not in line with *Ligue des droits humains*, as air carriers will have to transfer to the router API data in connection to all intra-EU flights, thus engaging with systematic, mass transfer.

- It is unclear whether there exists another alternative, whereby the selection of the intra-EU flights in line with the list provided by the Member States could take place at an earlier stage so that the transfer to the PIUs would be targeted, not merely the processing by the PIUs. A targeted impact assessment on this matter would have been necessary prior to tabling the API proposals.

- Considering the interaction of the router with certain interoperability components, particularly the CRRS, there exists a distinct danger of future function creep, whereby its operation could not be solely restricted in the transmission of API data. In particular, it is likely that the router may have a more important function in the future of border management and law enforcement by becoming the motor through which border authorities consult API data through the ESP, but the full picture is not clear just yet.

- In any case, the development of the router should be combined with strong security standards, such as encryption of the API data, so that it is guaranteed that eu-LISA does not have access to the API data transmitted.

- Any alternative solution whereby the selection of the API data will take place by the PIUs is also in violation of *Ligue des droits humains*.
- Clear assessment criteria for the collection and transfer of API data of intra-EU flights should be inserted either in the API law enforcement proposal or in a non-legislative act. These assessment criteria should not be imprecise and vague so that they can provide meaningful guidance to the Member States in selecting intra-EU flights.
- In line with *Ligue des droits humains*, the decision providing for application to intra-EU flights must be open to effective review either by a court or by an independent administrative body. In other words, the confidentiality creates opacity and to prevent this, it must be ensured that an independent administrative, parliamentary, and/or judicial oversight mechanism exists.
- Any extension of the scope of the API-related obligations to other modes of transport does not meet the tests of necessity and proportionality. The extension will affect millions or travellers, effectively creating a surveillance society. Furthermore, in relation to sea carriers, there already exist reporting requirements. Besides, in relation to land transport, the feasibility of introducing reporting obligations would disrupt the business model of carriers.
- The concept of non-scheduled flights must be clarified.
- The exclusion of transiting passengers must be clearly signposted in the legislation.
- The extension of the API data fields serves the alignment with international standards. Certain categories of API data, in particular those related to the seating and the baggage, could be more precise so that the list of API data will be closed, exhaustive and precise.
- The extension of the retention period of API data (both in relation to air carriers and to border authorities) has not been justified and is also not supported by the practices of most Member States in the domestic implementation of the API Directive.
- eu-LISA is rightly designated as a data processor and not as a data controller.
- Reference to the individual rights of travellers must be introduced.
- The relevant articles on supervision must be clarified; with regard to the API law enforcement proposal, the frequency of the audits must be specified. Furthermore, Article 29 of the API border management proposal has unclear content and is awkwardly worded.
- Inclusion of safeguards regarding the use of the statistical data retrieved from the CRRS by eu-LISA, so that they will not be used for risk analysis, profiling or predictive risk assessment, which may be to the detriment of travellers leading to discriminatory treatment.
- Specification of which agencies (in particular EDPS and FRA) will be involved in publication of the practical handbooks.
- Reconsideration whether the delegated acts should be implementing acts instead.

REFERENCES

- Evelien Brouwer, '*Ligue des Droits Humains* and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in times of new technologies' (Common Market Law Review, forthcoming 2023).
- Commission, 'Commission Staff Working Document – Impact Assessment Report accompanying the documents "Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC" "Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818"'SWD(2022) 422final.
- ______, 'Study supporting an impact assessment: potential effects of different possible measures on Advance Passenger Information' (2021).
- ______, 'A strategy towards a fully functioning and resilient Schengen area' (Communication) COM(2021) 277final.
- ______, Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SWD(2020) 128 final.
- ______, 'Staff Working Document – Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)' SWD(2020) 174 final.
- ______, 'Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data' (2020).
- ______, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205 final.
- ______, 'Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82' (2012).
- ______, 'Commission Staff Working Document – Impact Assessment Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime' COM(2011) 132final.
- Council, Document 7651/1/23 (13 April 2023).
- ______, Document 7753/23 (24 March 2023).
- ______, Document 7770/23 (23 March 2023).
- ______, Document 7327/1/23 (23 March 2023).
- ______, Document 5805/3/23 (21 March 2023).
- ______, Document 6853/1/23 (2 March 2023).
- ______, Document 6230/23 (13 February 2023).

- ______, Document 7829/16 (18 April 2016).
- EDPS, 'Opinion 6/2023 on the Proposals for Regulations on the collection and transfer of advance passenger information (API)'.
- European Border and Coast Guard Agency (EBGA), 'Report on API Systems and Targeting Centres (2018).
- European Council, 'G7 Taormina Statement on the fight against terrorism and violent extremism' (26 May 2017) https://www.consilium.europa.eu/en/press/press-releases/2017/05/26/statement-fight-against-terrorism/.
- ICAO, 'The World of Air Transport in 2019' https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx.
- ICAO, 'ICAO forecasts complete and sustainable recovery and growth of air passenger demand in 2023' (8 February 2023) https://www.icao.int/Newsroom/Pages/ICAO-forecasts-complete-and-sustainable-recovery-and-growth-of-air-passenger-demand-in-2023.aspx.
- Kuskonmaz E M, 'PNR Directive' in Violeta Moreno-Lax and Niovi Vavoula (eds), *Oxford Encyclopedia of European Union Law – Area of Freedom, Security and Justice* (Oxford University Press, forthcoming 2023).
- Kuskonmaz EM and Guild E, 'EU exclusive jurisdiction on surveillance related to terrorism and serious transnational crime, case review on opinion 1/15 of the CJEU' (2018) 43 *European Law Review* 583.
- Meijers Committee, 'Comment on the Legislative Proposals Providing for Collection and Transfer of Advance Passenger Information (API) (March 2023).
- Mitsilegas M, 'Contrôle des Etrangers, des Passagers, des Citoyens: Surveillance et Anti-terrorisme' (2005) 20 *Cultures & conflits* 185.
- ______, 'Interoperability as a Rule of Law Challenge' (Migration Policy Centre) https://migrationpolicycentre.eu/interoperability-as-a-rule-of-law-challenge/.
- OSCE, 'Ministerial Council Decision 6/16 of 9 December 2016 on Enhancing the use of Advance Passenger Information' https://www.osce.org/cio/288256.
- Thonnes C, 'A Directive Altered beyond Recognition - On the Court of Justice of the European Union's PNR decision (C-817/19)' (*Verfassungblog,* 23 June 2023) https://verfassungsblog.de/pnr-recognition/.
- Tzanou M, *The Fundamental Right to Data Protection -Normative Value in the Context of Counter-terrorism Surveillance* (Hart 2017).
- UN Security Council, Resolution 2178(2014) (24 September 2014).
- UN Security Council, Resolution 2309(2016) (22 September 2016).
- UN Security Council, Resolution 2396(2017) (21 December 2017).
- UN Security Council, Resolution 2482(2019) (19 July 2019).
- Vavoula N, *Immigration and Privacy in the Law of the European Union – The Case of Information Systems* (Brill 2022).

- ______, 'Police Information Exchange – The future development regarding Prüm and the API Directive' (Study commissioned by the LIBE Committee of the European Parliament, 2020).
- ______, 'The EU Response to the Phenomenon of Foreign Fighters: Challenges for Fundamental Rights and the Rule of Law' in Ulrich Sieber et al. (eds), *Alternative, Informal, and Transitional Types of Criminal Justice and the Legitimacy of New Sanction Models in the Global Risk Society* (Duncker & Humblot 2018).
- Vedaschi A, 'The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017' (2018) 14 *European Constitutional Law Review* 410.

Cases

- C-148/20 *AC v Deutsche Lufthansa AG*, OJ C 279/21.
- C-149/20 *DF v Deutsche Lufthansa SA*, OJ C279/21.
- C-150/20 *BD v Deutsche Lufthansa SA*, OJ C279/22.
- C-215/20 *JV v Bundesrepublik Deutschland*, OJ C 279/27.
- C-222/20 *OC v Bundesrepublik Deutschland*, OJ C 279/30.
- C-486/20 *Varuh človekovih pravic Republike Slovenije*, OJ C414/24.
- Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministers* ECLI:EU:C;2022:491.
- Opinion 1/15 ECLI:EU:C:2017:592.
- *Big Brother Watch v UK,* Appl nos 58170/13, 62322/14 and 24969/15 (Judgment of the Grand Chamber of 25 May 2021).
- *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to analyse the European Commission's proposals to reform the legal framework on the processing of Advance Passenger Information (API) data. The analysis takes stock of the current legal framework regarding the processing of travellers' data. Then, it provides an outline of the Commission's proposals, followed by an assessment of the fundamental rights implications, in particular the right to respect for private life (Article 7 of the EU Charter of fundamental rights), protection of personal data (Article 8) and freedom of movement (Article 45).

PE 745.768
IP/C/LIBE/IC/2023-009

Print ISBN 978-92-848-0786-4 | doi:10.2861/377168 | QA-03-23-225-EN-C
PDF ISBN 978-92-848-0787-1 | doi:10.2861/45240 | QA-03-23-225-EN-N