Council of the European Union

Brussels, 14 December 2022
(OR. en)

15719/22

Interinstitutional File: 2022/0425(COD)

IXIM 292
ENFOPOL 639
AVIATION 319
DATAPROTECT 363
JAI 1678
CODEC 2012
IA 223

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	14 December 2022
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2022) 731 final
Subject:	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

Delegations will find attached document COM(2022) 731 final.

Encl.: COM(2022) 731 final

EUROPEAN
COMMISSION

Strasbourg, 13.12.2022
COM(2022) 731 final

2022/0425 (COD)

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) 424 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Over the last decade the EU and other parts of the world have seen an increase in serious and organised crime. According to Europol's EU Serious and Organised Crime Threat Assessment, most organised crime involves international travel, typically aimed at smuggling persons, drugs or other illicit goods into the EU. Notably, criminals make frequent use of the EU's main airports as well as smaller regional airports operating low-cost airlines.[1] Likewise, Europol's Terrorism Situation and Trend Report shows that terrorist threat in the EU remains real and serious,[2] pointing out that most terrorist campaigns have a transnational character with either the involvement of either transnational contacts or travels outside the EU. In this context, information on air travellers is an important tool for law enforcement authorities to counter serious crime and terrorism in the EU.

Air traveller data includes Advance Passenger Information (API) and Passenger Name Records (PNR) which, when used together, are particularly effective to identify high-risk travellers and to confirm the travel pattern of suspected individuals. When a passenger buys a ticket with an air carrier, a PNR will be generated by the reservation systems of air carriers for their business purposes. This includes data on the complete itinerary, payment details, contact-details, and special requests of the passenger. Where an obligation to that effect applies, this PNR data is sent to the Passenger Information Unit (PIU) of the country of destination and often the country of departure.

In the EU, the PNR Directive[3] was adopted in 2016 to ensure that all Member States implement rules on collecting PNR data from air carriers to prevent, detect, investigate and prosecute terrorist offences and serious crime, without prejudice to existing EU rules on the obligation for air carriers to collect API data set in the API Directive.[4] Under the PNR Directive, Member States must adopt the necessary measures to ensure that air carriers transfer PNR data to the extent that they have already collected such data in the normal course of their business. The PNR Directive allows for the joint processing of both API data and PNR data, as its definition of PNR data includes 'any advance passenger information (API) data collected'.[5] However, the PNR Directive does not oblige air carriers to collect any data beyond the normal course of their business. Consequently, 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.

Only where an obligation to that effect applies, API data is collected by the air carrier during check-in of the passenger (online check-in and at the airport). It is then sent to competent border

---

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

2 Europol, Terrorism Situation and Trend Report (Te-SAT), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf.

3 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.

4 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

5 See point 18 of Annex 1 of Directive (EU) 2016/681.

authorities as a complete 'passenger list manifest' containing all passengers on board at departure of the plane. While API data are considered as 'verified' information as it corresponds to travellers which eventually boarded the aircraft, and which can also be used by law enforcement authorities to identify suspects and persons sought, PNR data is 'unverified' information provided by passengers. The PNR data of a certain passenger usually do not contain all potential PNR elements, but only those provided by the passenger and/or necessary for the booking and hence for the normal business purpose of the air carrier.

Since the adoption of the API Directive in 2004, there is global consensus that API data is not only a key instrument for border management, but also an important tool for law enforcement purposes, notably to counter serious crime and terrorism. Thus, at international level, since 2014, United Nations' Security Council Resolutions have repeatedly called for the establishment and global roll-out of API and PNR systems for law enforcement purposes.[6] In addition, the commitment by the Organization for Security and Co-operation in Europe (OSCE) participating states to set up API systems, confirm the importance of the use of this data in the fight against terrorism and transnational crime.[7]

As shown by the Commission's report on the PNR Directive review, the joint processing of API and PNR data by competent law enforcement authorities – meaning that the PNR data collected by air carriers for their normal business purposes and transferred to competent law enforcement authorities is complemented by an obligation on air carriers to collect and transfer API data – substantially increases the effectiveness of the fight against serious crimes and terrorism in the EU.[8] The combined use of API data and PNR data enables the competent national authorities to confirm the identity of passengers and greatly improves the reliability of PNR data. Such combined use prior to arrival also allows law enforcement authorities to conduct an assessment and perform a closer screening only of those persons who are most likely, based on objective assessment criteria and practices and in accordance with the applicable law, to pose a threat to security. This facilitates the travel of all other passengers and reduces the risk of passengers being subjected to examination upon arrival by the competent authorities based on discretionary elements such as race or ethnic origin which may wrongly be associated with security risks by law enforcement authorities.

However, the current EU legal framework only regulates the use of PNR data for fighting serious crime and terrorism but does not do so specifically for API data, which can be requested only on flights coming from third countries, leading to a security gap, notably regarding intra-EU flights for which Member States request air carriers to transfer PNR data. Passenger Information Units obtain the most effective operational results on flights where both API and PNR data are collected. This means that competent law enforcement authorities cannot benefit from the results of the joint processing of API data and PNR data on flights within the EU, for which only PNR data is transferred.

To address this gap, the Commission's June 2021 Strategy towards a fully functioning and resilient Schengen area called for an increased use of API data in combination with PNR data for intra-Schengen flights to significantly enhance internal security, in compliance with the

---

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

7 OSCE Ministerial Council Decision 6/16 of 9 December 2016 on Enhancing the use of Advance Passenger Information.

8 European Commission, Staff Working Document Accompanying the Report on the review of Directive 2016/681, SWD(2020)128 final.

fundamental right to the protection of personal data and the fundamental right to freedom of movement.[9]

The proposed Regulation therefore aims to lay down better rules for the collection and transfer of API data by air carriers for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime. In order to ensure compliance with the relevant fundamental rights enshrined in the Charter of Fundamental Rights of the EU ('Charter'), in particular the rights to privacy and to protection of personal data, and the resulting requirements of necessity and proportionality, the proposal is, as explained further below, carefully limited in scope and contains strict personal data protection limits and safeguards.

- **Consistency with existing policy provisions in the policy area**

The proposed rules on the collection and transfer of API data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime are aligned with the applicable rules for the processing of PNR data, as established in the PNR Directive.[10] They take account of the interpretations by the Court of Justice of the European Union in its recent case law, notably what is specified in that case law regarding the processing of PNR data for intra-EU flights, whereby the transfer of PNR data to Member States' competent authorities on intra-EU flights must be selective and cannot be systematic unless justified by a genuine and present or foreseeable terrorist threat.[11]

Insofar as there is a possible overlap between the proposed Regulation and the rules of the PNR Directive, considering that – as mentioned – under that Directive the definition of 'PNR data' includes 'any advance passenger information (API) data collected', the rules of the proposed Regulation prevail, considering that it is both *lex specialis* and *lex posterior*. While Member States must under the PNR Directive adopt the necessary measures to ensure that air carriers transfer PNR data to the extent that they have already collected such data in the normal course of their business, the proposed Regulation sets an obligation on air carriers to collect API data in specific situations and to transfer that data in a specific manner. The proposed Regulation therefore complements the PNR Directive, as it ensures that in all cases in which competent law enforcement authorities – i.e. the Passenger Information Units – receive PNR data under the PNR Directive, there is an obligation on air carriers to also collect and transfer API data to these competent authorities.

Following the transmission of API data to Passenger Information Units (PIUs) established by the PNR Directive, apart from the limited requirements in this regard as set out in the proposed Regulation, the rules on the subsequent processing of API data by the PIUs are those set out in the PNR Directive. As mentioned, the PNR Directive allows for the joint processing of API data and PNR data, as its definition of PNR data includes 'any advance passenger information (API) data collected', including therefore the API data received by PIUs pursuant to the proposed Regulation. Accordingly, the rules of Article 6 and Articles 9 and following of the PNR Directive apply, relating to matters such as the precise purposes of the processing, retention periods, deletion, exchange of information, transfer by the Member States to third countries and specific provisions on the protection of such personal data.

---

9 COM(2021) 277 final (2.6.2021).

10 PNR Directive sets conditions for the procession of the data such as the competent authorities involved (Article 7), period of data retention (Article 12) and protection of personal data (Article 13).

11 CJEU, iudgment in case Case C-817/19, *Ligue des droits humains*.

In addition, generally applicable acts of EU law will apply in accordance with the conditions set out therein. Where the processing of personal data is concerned, that holds true, in particular, for the General Data Protection Regulation (GDPR),[12] the data protection 'Law Enforcement Directive' (LED)[13] and the EU Data Protection Regulation[14]. Those acts are left unaffected by the present proposal.

The applicability of the abovementioned acts of EU law mean to the processing of the API data received under this Regulation mean that the Member States are implementing EU law within the meaning of Article 51(1) of the Charter, meaning that the rules of the Charter apply as well. In particular, the rules of those acts of EU law are to be interpreted in the light of the Charter.

Ensuring consistency with the rules laid down in the proposal for a Regulation on the collection and transfer of API data for border control purposes and efficiencies in the transmissions of API data, the present proposal provides for the obligation on air carriers to collect the same set of API data and transfer it to the same router established under that other proposed Regulation.

The collection of API data from travel documents is also consistent with the ICAO guidelines on Machine Readable Travel Documents,[15] that are transposed in Regulation 2019/1157 on strengthening the security of identity cards of Union citizens, Council Directive 2019/997 on EU emergency travel documents and Regulation 2252/2004 on standards for security features and biometrics in passports. These Regulations are the precursors to enable an automated extraction of complete and high-quality data from travel documents.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

For this proposed Regulation on the collection and transfer of API data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, having regard to its aim and the measures provided for, the appropriate legal basis is Articles 82(1)(d) and 87(2)(a) of the Treaty on the Functioning of the European Union (TFEU).

Under point (d) of paragraph 1 of Article 82 TFEU, the Union has the power to adopt measures relating to facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions. Under point (a) of paragraph 2 of Article 87 TFEU, the Union has the power to

---

12 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.

13 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.

14 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

15 ICAO, Document 9303, Machine Readable Travel Documents, Eigth Edition, 2021, available at: https://www.icao.int/publications/documents/9303_p1_cons_en.pdf.

adopt measures on the collection, storage, processing, analysis, and exchange of relevant information for the purposes of police cooperation in the EU.

Accordingly, the legal basis used for the present proposal is the same as the one used for the PNR Directive, which is appropriate considering not only that the proposed Regulation pursues essentially the same aim, but also that it seeks to complement the PNR Directive.

- **Subsidiarity**

Law enforcement authorities must be provided with effective tools to fight terrorism and serious crime. As most serious crimes and terrorist acts involve international travel, often by air, PNR data have proven to be very efficient to protect the internal security of the EU. Furthermore, investigations for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime carried out by the competent authorities of the Member States are largely dependent on international and cross-border cooperation.

In an area without internal border controls, collection, processing and exchange of passenger data, including PNR and API data, by Member States are also efficient compensatory measures. By acting coherently at EU level, the proposal will contribute to increasing the security of the Member States and, by extension, of the EU as a whole.

The API Directive is part of the Schengen *acquis* related to the crossing of the external borders. It therefore does not regulate the collection and transfer of API data on intra-EU flights. In the absence of API data to complement the PNR data for these flights, Member States have implemented a variety of different measures that seek to compensate the lack of identity data on the passengers. This includes physical conformity checks to verify identity data between travel document and boarding card that generate new issues without solving the underlying problem of not having API data.

Action at EU level will help to ensure the application of harmonised provisions on safeguarding fundamental rights, in particular personal data protection, in the Member States. The different systems of Member States that have already established similar mechanisms, or will do so in the future, may impact negatively on the air carriers as they may have to comply with several diverging national requirements, for example regarding the types of information to be transferred and the conditions under which this information needs to be provided to the Member States. These differences are prejudicial to effective cooperation between the Member States for the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime. Such harmonised rules can only be set at EU level.

Since the objectives of this proposal cannot be sufficiently achieved by the Member States, and can be better achieved at Union level, it can be concluded that the EU is both entitled to act and better placed to do so than the Member States acting independently. The proposal therefore complies with the subsidiarity principle as set out in Article 5 of the Treaty on European Union.

- **Proportionality**

According to the principle of proportionality laid down in Article 5(4) TEU, there is a need to match the nature and intensity of a given measure to the identified problem. All problems addressed in this legislative initiative call, in one way or another, for EU-level legislative action enabling Member States to tackle these problems effectively.

The proposed rules on the collection and transfer of API data, subject to strict limitations and safeguards, will strengthen the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Consequently, the proposed rules correspond to an identified need to enhance internal security, responding effectively to the problem resulting from the absence of joint processing of API data and PNR data, including on those intra-EU flights for which Member States receive PNR data.

The scope of the proposal is limited to what is strictly necessary, i.e. it is limited to those elements that require a harmonised EU approach, namely the purposes for which API can be used by the Passenger Information Units, the data elements that need to be collected and the means for the collection and transfer of the API data from travellers. The transfer of the API data to the router reduces the complexity for air carriers to maintain connections with Passenger Information Units and introduces economies of scale, whilst reducing the scope for errors and abuse. The purpose covers only terrorist offences and serious crime, as defined in the proposal, in view of the serious nature thereof and their transnational dimension.

To limit the interference on the rights of passengers to what is strictly necessary, a number of safeguards are set out in the proposal. More specifically, the processing of API data under the proposed Regulation is restricted to a closed and limited list of API data. Beyond that, no additional identity data are to be collected. Moreover, the proposed Regulation only provides for rules on the collection and transfer of API data through the router to the PIUs for the limited purposes specified therein and does not regulate the further processing of API data by the PIUs, given that, as explained above, that is covered by other acts of EU law (PNR Directive, personal data protection law, the Charter). The functionalities of the router and in particular its capability to collect and provide comprehensive statistical information also supports the monitoring of the implementation of this Regulation by air carriers and Passenger Information Units. Certain specific safeguards are also provided for, such as rules on logging, personal data protection and security.

To ensure the necessity and proportionality of the data processing under the proposed Regulation, and more specifically as regards the collection and transfer of API data on intra-EU flights, Member States will only receive API data for those intra-EU flights that they have selected in line with the abovementioned case law of the CJEU. In addition, the further processing of API data by PIUs would be subject to the limits and safeguards established in the PNR Directive, as interpreted by the CJEU in the *Ligue des droits humains* case[16] in the light of the Charter.

- **Choice of the instrument**

The proposed action is a Regulation. In view of the need for the proposed measures to be directly applicable and uniformly applied across Member States, a Regulation is therefore the appropriate choice of legal instrument.

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

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

• Ex-post evaluation of existing legislation

The API Directive does not prevent the processing of API data for law enforcement purposes as provided in national legislation and subject to personal data protection requirements. However, the implementation of this possibility across Member States is problematic, as found by the evaluation of the API Directive, leading to security gaps due a lack of EU-defined criteria on the collection and transfer of API for law enforcement purposes:[17]

– The law enforcement purpose is construed widely in some Member States' national laws, ranging from administrative offences, enhancing internal security and public order, to fight against terrorism and safeguarding national security interests. The API Directive evaluation also indicated that an effective use of API data for law enforcement would require a dedicated legal instrument for this distinct purpose.[18]

– The variety of purposes for collecting API data adds complexity to ensuring compliance with the EU's personal data protection framework. The requirement to delete API data within 24 hours is established only in the case of the use of API data for the principal aim of the API Directive, namely external border management. It is not clear whether this requirement also applies in respect of processing conducted for law enforcement purposes.

– The API data set that can be requested from carriers for law enforcement purposes, in addition to the practice of some Member States to request API data going beyond the non-exhaustive list included in the API Directive, create additional hindrances for air carriers to comply with the different requirements when transporting passengers to the EU.

– Likewise, the API Directive gives no indications of the flights for which API data can be requested nor to which authority API data should be transferred or conditions of access to such data for law enforcement purposes.

• Stakeholder consultations

The preparation of this proposal involved a wide range of consultations of concerned stakeholders, including Member States' authorities (competent border authorities, Passenger Information Units), transport industry representatives and individual carriers. EU agencies – such as the European Border and Coast Guard Agency (Frontex), the EU Agency for Law Enforcement Cooperation (Europol), the EU Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice (eu-LISA) and the EU Agency for Fundamental Rights (FRA), also provided input. This initiative also integrates the views and feedback received during the public consultation carried out end of 2019 within the framework of the evaluation of the API Directive.[19]

---

17 European Commission, Staff Working Document, Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), Brussels, 8.9.2020, SWD(2020)174 final, pp. 26, 43.

18 SWD(2020)174, p. 57.

19 SWD(2020)174.

Consultation activities in the context of the preparation of the impact assessment supporting this proposal gathered feedback from stakeholders using various methods. These activities included notably an inception impact assessment, an external supporting study and a series of technical workshops.

An inception impact assessment was published for feedback from 5 June 2020 to 14 August 2020, with a total of seven contributions received providing feedback on the extension of the scope of the future API Directive, data quality, sanctions, relation of API data and PNR data, and protection of personal data.[20]

The external supporting study was conducted based on desk research, interviews and surveys with subject matter experts which examined different possible measures for the processing of API data with clear rules that facilitate legitimate travel, are consistent with interoperability of EU information systems, EU personal data protection requirements, and other existing EU instruments and international standards.

The Commission services also organised a series of technical workshops with experts from Member States and Schengen Associated Countries. These workshops aimed at bringing together experts for an exchange of views on the possible options which were envisaged to strengthen the future API framework for border management purposes, and also for fighting crime and terrorism.

The accompanying impact assessment sets out a more detailed description of the stakeholder consultation (Annex 2).

- **Impact assessment**

In line with the Better Regulation Guidelines, the Commission conducted an Impact Assessment, as presented in the accompanying Staff Working document [reference]. The Regulatory Scrutiny Board reviewed the draft impact assessment at its meeting of 28 September 2022 and delivered its positive opinion on 30 September 2022.

In view of the problems identified on the collection and transfer of API data, the Impact Assessment evaluated policy options on the scope of collection of API data for external border management and for law enforcement purposes, together with options on the means to improving the quality of API data. As regards the collection of API data for law enforcement purposes, the impact assessment considered the collection of API data on all extra-EU flights on the one hand, and the collection of API data on all extra-EU and on selected intra-EU flights on the other hand. In addition, the Impact Assessment also considered options to improve the quality of API data – either to collect API data using automated and manual means, or to collect API data using automated means only.

Based on the findings of the Impact Assessment report, the preferred option for an API instrument for law enforcement purposes includes the collection of API data on all flights into and outside the EU, as well as on selected intra-EU flights for which PNR data is transferred. This will significantly reinforce the robustness of the necessary analysis of relevant data relating to air travellers in the fight against serious crime and terrorism, with Passenger Information Units benefitting from the availability of API data, verified and hence of a higher

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

quality, in order to identify persons involved in serious crime or terrorism. The collection and transfer of API data for law enforcement purposes builds on the capabilities developed for the transfer of API data, via the router, for external border management, with no additional costs for eu-LISA. Air carriers transfer API data only to the router, which would then transmit that data to the Passenger Information Unit of each Member State concerned. The impact assessment concluded this to be a cost-efficient solution for air carriers, bringing down part of the transmission costs incurred by air carriers, whilst also limiting the scope for errors or abuse. However, different from the current situation, under the proposed Regulation air carriers would need to collect and transfer API data on all flights covered, irrespective of their normal business needs and including also intra-EU flights. The proposal is consistent with the climate-neutrality objective set out in the European Climate Law[21] and the Union 2030 and 2040 targets.

- **Fundamental rights**

This initiative provides for the processing of personal data of travellers and therefore limits the exercise of the fundamental right to the protection of personal data as guaranteed by Article 8 of the Charter and Article 16 of the TFEU. As underlined by the Court of Justice of the EU (CJEU),[22] the right to the protection of personal data is not an absolute right, but any limitation must be considered in relation to its function in society and comply with the criteria set out in Article 52(1) of the Charter.[23] Personal data protection is also closely linked to respect for the right to privacy, as part of the right to private and family life protected by Article 7 of the Charter.

When it comes to the collection and transfer of API data for selected intra-EU flights, this initiative also affects the exercise of the fundamental right to freedom of movement provided for by Article 45 of the Charter and Article 21 of the TFEU. According to the CJEU, an obstacle to the freedom of movement of persons can be justified only where it is based on objective considerations and is proportionate to the legitimate objective of the national provisions[24].

Under this Regulation, the collection and transfer of API data can only be for the prevention, detection, investigation and prosecution of terrorism and serious crime, as defined by the PNR Directive. The provisions in this proposal provide for uniform criteria for the collection and transfer of API data on extra-EU flights (inbound and outbound) on the one hand and selected intra-EU flights on the other hand, based on an assessment carried out by Member States and subject to regular review, in line with the requirements set by the the Court of Justice in the *Ligue des droits humains* case. The obligation on the air carriers to collect and transfer API data to the router covers all intra-EU flights. The transmission by the router to the PIUs is a technical solution to limit the transmission of API data to Passenger Information Units to selected flights only, without disclosing confidential information on which intra-EU flights

---

21 Article 2(1) of Regulation (EU) 2021/1119 of 30 June 2021 establishing the framework for achieving climate neutrality (European Climate Law).

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

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

24 CJEU, judgment of 5 June 2018, Case C-673/16, *Coman*.

have been selected. Such information is to be treated confidentially, in view of the risk of circumvention that would exist should it become known to the general public or, more specifically, to persons involved in serious crime or terrorist activities.

The mandatory use of automated means by air carriers to collect certain API data from travellers can lead to risks, including from the viewpoint of the protection of personal data. However, such risks have been limited and mitigated. Firstly, the requirement applies only in respect of certain API data, where automated means can be used responsibly, i.e. for machine-readable data on travellers' documents. Secondly, the proposed Regulation contains requirements regarding the automated means to be used, which are to be elaborated further in a delegated act. Finally, several safeguards are provided for, such as logging, specific rules on the protection of personal data and effective supervision.

Furthermore, whilst – apart from the provision ensuring compliance with the principle of purpose limitation – the proposed Regulation would not regulate the use that the competent border authorities make of the API data that they receive thereunder given that – as explained above – that is already covered by other legislation, in the interest of clarity it is recalled in the recitals that any such use may not lead to any discrimination precluded under Article 21 of the Charter.

4. BUDGETARY IMPLICATIONS

This legislative initiative on the collection and transfer of API data, respectively, for facilitating external border controls and for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, would have an impact on the budget and staff needs of eu-LISA and Member States' competent authorities.

For eu-LISA, it is estimated that an additional budget of around EUR 45 million (33 million under current MFF) to set-up the router and EUR 9 million per year from 2029 onwards for the technical management thereof, and that around 27 additional posts would be needed for to ensure that eu-LISA has the necessary resources to perform the tasks attributed to it in this proposed Regulation and the proposed Regulation on the collection and transfer of API data for facilitating external border controls.

For Member States, it is estimated that EUR 11 million (EUR 3 million under the current Multiannual Financial Framework) dedicated to upgrading the necessary national systems and infrastructures for the PIUs could be entitled for reimbursement by the Internal Security Fund[25], and from 2028 onwards, progressively up to an estimated EUR 2 million per year. Any such entitlement will ultimately have to be determined in accordance with the rules regulating those funds as well as the rules on costs contained in the proposed Regulation.

In view of the close connection between this proposed Regulation and the proposed Regulation on the collection and transfer of API data for facilitating external border controls, particularly as regards the transfer of API data to the router, the legislative financial statement, in annex of this proposed Regulation, is identical to both proposals.

[25] Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

The Commission would ensure that the necessary arrangements are in place to monitor the functioning of the measures proposed and evaluate them against the main policy objectives. Four years after the commencement of operations of the proposed API Regulation, and every four years thereafter, the Commission would submit a report to the European Parliament and the Council assessing the implementation of the Regulation and its added value. The report would also report on any direct or indirect impact on fundamental rights. It would examine results achieved against objectives and assess the continuing validity of the underlying rationale and any implications for future options.

The mandatory nature of the obligation for air carriers to collect API data on extra-EU and selected intra-EU flights and the introduction of the API router will allow for a clearer view on both the transmission of API data by air carriers and the use of API data by Member States in accordance with applicable national and Union legislation. This will support the Commission in its evaluation and enforcement tasks by providing it with reliable statistics on the volume of data transmitted and on the flights for which API data would be requested.

• Detailed explanation of the specific provisions of the proposal

Chapter 1 sets out the general provisions for this Regulation, starting with rules on its subject matter and scope. It also contains a list of definitions.

Chapter 2 sets out the provisions for the collection, transfer to the router and deletion of API data by air carriers, and rules regarding the transmission of API data from the router to the Passenger Information Units.

Chapter 3 contains specific provisions on logs, specifications as to whom are the personal data controllers in relation to processing of API data constituting personal data under this Regulation, security and self-monitoring by air carriers and PIUs.

Chapter 4 further sets out rules on the connections to, and integration with, the router by Passenger Information Units and air carriers, as well as on Member States' costs in connection thereto. It also contains provisions regulating the situation of a partial or full technical impossibility to use the router and on liability for damage caused to the router.

Chapter 5 contains provisions on supervision, on possible penalties applicable to air carriers for non-compliance of their obligations set out in this Regulation and on the preparation of a practical handbook by the Commission.

Chapter 6 provides for amendments to other existing instruments, i.e. Regulation (EU) 2019/818.

Chapter 7 contains the final provisions of this Regulation, which concern the adoption of delegated acts, the monitoring and evaluation of this Regulation, and its entry into force and application.

2022/0425 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1), point (d), and Article 87(2), point (a), thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[26],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The transnational dimension of serious and organised crime and the continuous threat of terrorist attacks on European soil call for action at Union level to adopt appropriate measures to ensure security within an area of freedom, security and justice without internal borders. Information on air travellers, such as Passenger Name Records (PNR) and in particular Advance Passenger Information (API), is essential in order to identify high-risk travellers, including those who are not otherwise known to law enforcement authorities, and to establish links between members of criminal groups, and countering terrorist activities.

(2) While Council Directive 2004/82/EC[27] establishes a legal framework for the collection and transfer of API data by air carriers with the aims of improving border controls and combating illegal immigration, it also states that Member States may use API data for law enforcement purposes. However, only creating such a possibility leads to several gaps and shortcomings. In particular, it means that, despite its relevance for law enforcement purposes, API data is not in all cases collected and transferred by air carriers for those purposes. It also means that, where Member States acted upon the possibility, air carriers are faced with diverging requirements under national law as regards when and how to collect and transfer API data for this purpose. Those divergences lead not only to unnecessary costs and complications for the air carriers,

[26] OJ C , , p. .

[27] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

but they are also prejudicial to the Union's internal security and effective cooperation between the competent law enforcement authorities of the Member States. Moreover, in view of the different nature of the purposes of facilitating border controls and law enforcement, it is appropriate to establish a distinct legal framework for the collection and transfer of API data for each of those purposes.

(3) Directive (EU) 2016/681 of the European Parliament and of the Council[28] lays down rules on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Under that Directive, Member States must adopt the necessary measures to ensure that air carriers transfer PNR data, including any API data collected, to the national Passenger Information Unit ('PIU') established under that Directive to the extent that they have already collected such data in the normal course of their business. Consequently, that Directive does not guarantee the collection and transfer of API data in all cases, as air carriers do not have any business purpose to collect a full set of such data. Ensuring that PIUs receive API data together with PNR data is important, since the joint processing of such data is needed for the competent law enforcement authorities of the Member States to be able to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime. In particular, such joint processing allows for the accurate identification of those passengers that may need to be further examined, in accordance with the applicable law, by those authorities. In addition, that Directive does not specify in detail which information constitutes API data. For those reasons, complementary rules should be established requiring air carriers to collect and subsequently transfer a specifically defined set of API data, which requirements should apply to the extent that the air carriers are bound under that Directive to collect and transfer PNR data on the same flight.

(4) It is therefore necessary to establish at Union level clear, harmonised and effective rules on the collection and transfer of API data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

(5) Considering the close relationship between both acts, this Regulation should be understood as complementing the rules provided for in Directive (EU) 2016/681. Therefore, API data is to be collected and transferred in accordance with the specific requirements of this Regulation, including as regards the situations and the manner in which that is to be done. However, the rules of that Directive apply in respect of matters not specifically covered by this Regulation, especially the rules on the subsequent processing of the API data received by the PIUs, exchange of information between Member States, conditions of access by the European Union Agency for Law Enforcement Cooperation (Europol), transfers to third countries, retention and depersonalisation, as well as the protection of personal data. Insofar as those rules apply, the rules of that Directive on penalties and the national supervisory authorities apply as well. This Regulation should leave those rules unaffected.

(6) 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

[28] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

data, in accordance with the Charter of Fundamental Rights of the European Union ('Charter'), adequate limits and safeguards should be provided for. In particular, any processing of API data and, in particular, API data constituting personal data, should remain limited to what is necessary for and proportionate to achieving the objectives pursued by this Regulation. In addition, it should be ensured that the API collected and transferred under this Regulation do not lead to any form of discrimination precluded by the Charter.

(7) In view of the complementary nature of this Regulation in relation to Directive (EU) 2016/681, the obligations of air carriers under this Regulation should apply in respect of all flights for which Member States are to require air carriers to transmit PNR data under Directive (EU) 2016/681, namely flights, including both scheduled and non-scheduled flights, both between Member States and third countries (extra-EU flights), and between several Member States (intra-EU flights) insofar as those flights have been selected in accordance with Directive (EU) 2016/681, irrespective of the place of establishment of the air carriers conducting those flights.

(8) Accordingly, given that Directive (EU) 2016/681 does not cover domestic flights, that is, flights that depart and land on the territory of the same Member State without any stop-over in the territory of another Member State or a third country, and in view of the transnational dimension of the terrorist offences and the serious crime covered by this Regulation, such flights should not be covered by this Regulation either. This Regulation should not be understood as affecting the possibility for Member States to provide, under their national law and in compliance with Union law, for obligations on air carriers to collect and transfer API data on such domestic flights.

(9) In view of the close relationship between the acts of Union law concerned and in the interest of consistency and coherence, the definitions set out in this Regulation should as much possible be aligned with, and be interpreted and applied in the light of, the definitions set out in Directive (EU) 2016/681 and Regulation (EU) [API border management][29].

(10) In particular, the items of information that jointly constitute the API data to be collected and subsequently transferred under this Regulation should be those listed clearly and exhaustively in Regulation (EU) API [border management], covering both information relating to each passenger and information on the flight of that traveller. Under this Regulation, such flight information should cover information on the border crossing point of entry into the territory of the Member State concerned only where applicable, that is, not when the API data relate to intra-EU flights.

(11) In order to ensure a consistent approach on the collection and transfer of API data by air carriers as much as possible, the rules set out in this Regulation should be aligned with those set out in the Regulation (EU) [API border management] where appropriate. That concerns, in particular, the rules on data quality, the air carriers' use of automated means for such collection, the precise manner in which they are to transfer the collected API data to the router and the deletion of the API data.

[29] OJ C , , p. .

(12) In order to ensure the joint processing of API data and PNR data to effectively fight terrorism and serious crime in the Union and at the same time minimise the interference with passengers' fundamental rights protected under the Charter, the PIUs should be the competent authorities in the Member States that are entrusted to receive, and subsequently further process and protect, API data collected and transferred under this Regulation. In the interest of efficiency and to minimise any security risks, the router, as designed, developed, hosted and technically maintained by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) in accordance with Regulation (EU) [API border management], should transmit the API data, collected and transferred to it by the air carriers under this Regulation, to the relevant PIUs. Given the necessary level of protection of API data constituting personal data, including to ensure the confidentiality of the information concerned, the API data should be transmitted by the router to the relevant PIUs in an automated manner.

(13) For extra-EU flights, the PIU of the Member State on the territory of which the flight will land and or from the territory of which the flight will depart should receive the API data from the router for all those flights, given that that PNR data is collected for all those flights in accordance with Directive (EU) 2016/681. The router should identify the flight and the corresponding PIUs using the information contained in the PNR record locator, a data element common to both the API and PNR data sets allowing for the joint processing of API data and PNR data by the PIUs.

(14) As regards intra-EU flights, in line with the case law of the Court of Justice of the European Union (CJEU), in order to avoid unduly interfering with the relevant fundamental rights protected under the Charter and to ensure compliance with the requirements of Union law on the free movement of persons and the abolition of internal border controls, a selective approach should be provided for. In view of the importance of ensuring that API data can be processed together with PNR data, that approach should be aligned with that of Directive (EU) 2016/681. For those reasons, API data on those flights should only be transmitted from the router to the relevant PIUs, where the Member States have selected the flights concerned in application of Article 2 of Directive (EU) 2016/681. As recalled by the CJEU, the selection entails Member States targeting the obligations in question only at, inter alia, certain routes, travel patterns or airports, subject to the regular review of that selection.

(15) In order to enable the application of that selective approach under this Regulation in respect of intra-EU flights, the Member States should be required to draw up and submit to eu-LISA the lists of the flights they selected, so that eu-LISA can ensure that only for those flights API data is transmitted from the router to the relevant PIUs and that the API data on other intra-EU flights is immediately and permanently deleted.

(16) In order not to endanger the effectiveness of the system that relies on the collection and transfer of API data set up by this Regulation, and of PNR data under the system set up by Directive (EU) 2016/681, for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, in particular by creating the risk of circumvention, information on which intra-EU flights the Member States selected should be treated in a confidential manner. For that reason, such information should not be shared with the air carriers and they should therefore be required to collect API data on all flights covered by this Regulation, including all intra-EU flights, and then transfer it to the router, where the necessary selection should

be enacted. Moreover, by collecting API data on all intra-EU flights, passengers are not made aware on which selected intra-EU flights API data, and hence also PNR data, is transmitted to PIUs in accordance with Member States' assessment. That approach also ensures that any changes relating to that selection can be implemented swiftly and effectively, without imposing any undue economic and operational burdens on the air carriers.

(17) In the interest of ensuring compliance with the fundamental right to protection of personal data and in line with Regulation (EU) [API border management], this Regulation should identify the controllers. In the interest of effective monitoring, ensuring adequate protection of personal data and minimising security risks, rules should also be provided for on logging, security of processing and self-monitoring. Where they relate to the processing of personal data, those provisions should be understood as complementing the generally applicable acts of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[30], Directive (EU) 2016/680 of the European Parliament and the Council[31] and Regulation (EU) 2018/1725 of the European Parliament and the Council[32]. Those acts, which also apply to the processing of personal data under this Regulation in accordance with the provisions thereof, should not be affected by this Regulation.

(18) The router to be created and operated under Regulation (EU) [API border management] should reduce and simplify the technical connections needed to transfer API data, limiting them to a single connection per air carrier and per PIU. Therefore, this Regulation provides for the obligation for the PIUs and air carriers to each establish such a connection to, and achieve the required integration with, the router, so as to ensure that the system for transferring API data established by this Regulation can function properly.

(19) In view of the Union interests at stake, appropriate costs incurred by the Member States in relation to their connections to, and integration with, the router, as required under this Regulation, should be borne by the Union budget, in accordance with the applicable legislation and subject to certain exceptions. The costs covered by those exceptions should be borne by each Member State concerned itself.

(20) In accordance with Regulation (EU) 2018/1726, Member States may entrust eu-LISA with the task of facilitating connectivity with air carriers in order to assist Member

---

30 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), OJ L 119, 4.5.2016, p. 1.

31 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, OJ L 119, 4.5.2016, p. 89.

32 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39

States in the implementation of Directive (EU) 2016/681, particularly by collecting and transferring PNR data via the router.

(21) It cannot be excluded that, due to exceptional circumstances and despite all reasonable measures having been taken in accordance with this Regulation and, as regards the router, Regulation (EU) [API border management], the router or the systems or infrastructure connecting the PIUs and the air carriers thereto fail to function properly, thus leading to a technical impossibility to use the router to transmit API data. Given the unavailability of the router and that it will generally not be reasonably possible for air carriers to transfer the API data affected by the failure in a lawful, secure, effective and swift manner through alternative means, the obligation for air carriers to transfer that API data to the router should cease to apply for as long as the technical impossibility persist. In order to minimise the duration and negative consequences thereof, the parties concerned should in such a case immediately inform each other and immediately take all necessary measures to address the technical impossibility. This arrangement should be without prejudice to the obligations under this Regulation of all parties concerned to ensure that the router and their respective systems and infrastructure function properly, as well as the fact that air carriers are subject to penalties when they fail to meet those obligations, including when they seek to rely on this arrangement where such reliance is not justified. In order to deter such abuse and to facilitate supervision and, where necessary, the imposition of penalties, air carriers that rely on this arrangement on account of the failure of their own system and infrastructure should report thereon to the competent supervisory authority.

(22) In order to ensure that the rules of this Regulation are applied effectively by air carriers, provision should be made for the designation and empowerment of national authorities charged with the supervision of those rules. The rules of this Regulation on such supervision, including as regards the imposition of penalties where necessary, should leave the tasks and powers of the supervisory authorities established in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 unaffected, including in relation to the processing of personal data under this Regulation.

(23) Effective, proportionate and dissuasive penalties, including financial ones, should be provided for by Member States against those air carriers failing to meet their obligations regarding the collection and transfer of API data under this Regulation.

(24) In order to adopt measures relating to the technical requirements and operational rules for the automated means for the collection of machine-readable API data, to the common protocols and formats to be used for the transfer of API data by air carriers, to the technical and procedural rules for the transmission of API data from the router and to the PIUs and to the PIU's and air carriers' connections to and integration with the router, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of Articles 4, 5, 10 and 11, respectively. It 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[33]. In particular, to ensure equal participation in the preparation of delegated

[33] OJ L 123, 12.5.2016, p. 1.

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.

(25) All interested parties, and in particular the air carriers and the PIUs, should be afforded sufficient time to make the necessary preparations to be able to meet their respective obligations under this Regulation, taking into account that some of those preparations, such as those regarding the obligations on the connection to and integration with the router, can only be finalised when the design and development phases of the router have been completed and the router starts operations. Therefore, this Regulation should apply only from an appropriate date after the date at which the router starts operations, as specified by the Commission in accordance with Regulation (EU) [API border management]. However, it should be possible for the Commission to adopt delegated acts under this Regulation already from an earlier date, so as to ensure that the system set up by this Regulation is operational as soon as possible.

(26) The objectives of this Regulation, namely contributing to the prevention, detection, investigation and prosecution of terrorist offences and serious crime, in view of the transnational dimension of the offences concerned and the need to cooperate on a cross-border basis to effectively address them, cannot be sufficiently achieved by the Member States individually, but can rather be better achieved at Union level. The Union may therefore adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(27) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(28) [In accordance with Article 3 of the Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation.] OR [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]

(29) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on [XX].[34]

[34] [OJ C …]

HAVE ADOPTED THIS REGULATION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

For the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, this Regulation lays down the rules on:

(a) the collection by air carriers of advance passenger information data ('API data') on extra EU flights and selected intra EU flights;

(b) the transfer by air carriers to the router of the API data;

(c) the transmission from the router to the Passenger Information Units ('PIUs') of the API data on extra-EU flights and selected intra-EU flights.

Article 2

Scope

This Regulation applies to air carriers conducting scheduled or non-scheduled extra-EU flights or intra-EU flights.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(a) 'air carrier' means an air transport undertaking as defined in Article 3, point (1), of Directive (EU) 2016/681;

(b) 'extra-EU flights' means any flight as defined in Article 3, point (2), of Directive (EU) 2016/681;

(c) 'intra-EU flight' means any flight as defined in Article 3, point (3), of Directive (EU) 2016/681;

(d) 'scheduled flight' means a flight as defined in Article 3, point (e), of Regulation (EU) [API border management];

(e) 'non-scheduled flight' means a flight as defined in Article 3, point (f), of Regulation (EU) [API border management];

(f) ‘passenger’ means any person as defined in Article 3, point (4), of Directive (EU) 2016/681;

(g) ‘crew’ means any person as defined in Article 3, point (h), of Regulation (EU) [API border management];

(h) ‘traveller’ means any person as defined in Article 3, point (i), of Regulation (EU) [API border management];

(i) ‘advance passenger information data’ or ‘API data’ means the data as defined in Article 3, point (j), of Regulation (EU) [API border management];

(j) ‘passenger name record’ or 'PNR' means a record of each passenger’s travel requirements as defined in Article 3, point (5), of Directive (EU) 2016/681;

(k) ‘Passenger Information Unit’ or ‘PIU’ means the competent authority established by a Member State, as contained in the notifications and modifications published by the Commission pursuant to Article 4(1) and (5), respectively, of Directive (EU) 2016/681;

(l) ‘terrorist offences’ means the offences as defined in Articles 3 to 12 of Directive (EU) 2017/541 of the European Parliament and the Council[35];

(m) ‘serious crime’ means the offences as defined in Article 3, point (9), of Directive 2016/681;

(n) ‘the router’ means the router as defined in Article 3, point (k) of Regulation (EU) [API border management];

(o) ’personal data’ means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679.

CHAPTER 2

PROCESSING OF API DATA

Article 4

Collection, transfer and deletion of API data by air carriers

1. Air carriers shall collect API data of travellers on the flights referred to in Article 2, for the purpose of transferring that API data to the router in accordance with

[35] 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 (OJ L 88, 31.3.2017, p. 6).

paragraph 6. Where the flight is code-shared between one or more air carriers, the obligation to transfer the API data shall be on the air carrier that operates the flight.

2. Air carriers shall collect the API data in such a manner that the API data that they transfer in accordance with paragraph 6 is accurate, complete and up-to-date.

3. Air carriers shall collect the API data referred to Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means to collect the machine-readable data of the travel document of the traveller concerned. They shall do so in accordance with the detailed technical requirements and operational rules referred paragraph 5, where such rules have been adopted and are applicable.

However, where such use of automated means is not possible due to the travel document not containing machine-readable data, air carriers shall collect that data manually, in such a manner as to ensure compliance with paragraph 2.

4. Any automated means used by air carriers to collect API data under this Regulation shall be reliable, secure and up-to-date.

5. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down detailed technical requirements and operational rules for the collection of the API data referred to in Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means in accordance with paragraphs 3 and 4 of this Article.

6. Air carriers shall transfer the API data collected pursuant to paragraph 1 to the router, by electronic means. They shall do so in accordance with the detailed rules referred to in paragraph 9, where such rules have been adopted and are applicable.

7. Air carriers shall transfer the API data both at the moment of check-in and immediately after flight closure, that is, once the travellers have boarded the aircraft in preparation for departure and it is no longer possible for travellers to board or to leave the aircraft.

8. 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, air carriers shall immediately either correct, complete or update, or permanently delete, the API data concerned in both of the following situations:

(a) where they become aware that the API data collected is inaccurate, incomplete or no longer up-to-date or was processed unlawfully, or that the data transferred does not constitute API data;

(b) where the transfer of the API data in accordance with paragraph 3 has been completed.

Where the air carriers obtain the awareness referred to in point (a) of the first subparagraph of this paragraph after having completed the transfer of the data in accordance with paragraph 6, they shall immediately inform the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). Upon receiving such information, eu-LISA

shall immediately inform the PIUs that received the API data transmitted through the router.

9. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying 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 referred to in paragraph 6.

Article 5

Transmission of API data from the router to the PIUs

1. The router shall, immediately and in an automated manner, transmit the API data, transferred to it by air carriers pursuant to Article 4, to the PIUs 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 the case of intra-EU-flights. Where a flight has one or more stop-overs at the territory of other Member States than the one from which it departed, the router shall transmit the API data to the PIUs of all the Member States concerned.

   For the purpose of such transmission, eu-LISA shall establish and keep up-to-date a table of correspondence between the different airports of origin and destination and the countries to which they belong

   However, for intra-EU flights, the router shall only transmit the API data to that PIU in respect of the flights included in the list referred to in paragraph 2.

The router shall transmit the API data in accordance with the detailed rules referred to in paragraph 3, where such rules have been adopted and are applicable.2. Member States that decide to apply Directive (EU) 2016/681 to intra-EU flights in accordance with Article 2 of that Directive shall each establish a list of the intra-EU flights concerned and shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, provide eu-LISA with that list. Those Member States shall, in accordance with Article 2 of that Directive, regularly review and where necessary update those lists and shall immediately provide eu-LISA with any such updated lists. The information contained on those lists shall be treated confidentially.

3. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

CHAPTER 3

LOGGING, PERSONAL DATA PROTECTION AND SECURITY

Article 6

Keeping of logs

1. Air carriers shall create logs of all processing operations under this Regulation undertaken using the automated means referred to in Article 4(3). Those logs shall cover the date, time, and place of transfer of the API data.

2. The logs referred to in paragraph 1 shall be used only for ensuring the security and integrity of the API data and the lawfulness of the processing, in particular as regards compliance with the requirements set out in this Regulation, including proceedings for penalties for infringements of those requirements in accordance with Articles 15 and 16.

3. Air carriers shall take appropriate measures to protect the logs that they created pursuant to paragraph 1 against unauthorised access and other security risks.

4. Air carriers shall keep the logs that they created pursuant to paragraph 1, for a time period of one year from the moment of the creation of those logs. They shall immediately and permanently delete those logs upon the expiry of that time period.

   However, if those logs are needed for procedures for monitoring or ensuring the security and integrity of the API data or the lawfulness of the processing operations, as referred to in paragraph 2, and those procedures have already begun at the moment of the expiry of the time period referred to in the first subparagraph, air carriers may keep those logs for as long as necessary for those procedures. In that case, they shall immediately delete those logs when they are no longer necessary for those procedures.

Article 7

Personal data controllers

The PIUs shall be controllers, within the meaning of Article 3, point (8), of Directive (EU) 2016/680 in relation to the processing of API data constituting personal data under this Regulation through the router, including transmission and storage for technical reasons of that data on the router.

The air carriers shall be controllers, within the meaning of Article 4, point (7), of Regulation (EU) 2016/679, for the processing of API data constituting personal data in relation to their collection of that data and their transfer thereof to the router under this Regulation.

Article 8

Security

PIUs and air carriers shall ensure the security of the API data, in particular API data constituting personal data, that they process pursuant to this Regulation.

PIUs and air carriers shall cooperate, in accordance with their respective responsibilities and in compliance with Union law, with each other and with eu-LISA to ensure such security.

Article 9

Self-monitoring

Air carriers and the PIUs shall monitor their compliance with their respective obligations under this Regulation, in particular as regards their processing of API data constituting personal data, including through frequent verification of the logs in accordance with Article 7.

CHAPTER 4

MATTERS RELATING TO THE ROUTER

Article 10

PIUs' connections to the router

1. Member States shall ensure that their PIUs are connected to the router. They shall ensure that their national systems and infrastructure for the reception and further processing of API data transferred pursuant to this Regulation are integrated with the router.

   Member States shall ensure that the connection to that router and integration with it enables their PIUs to receive and further process the API data, as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner.

2. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 11

Air carriers' connections to the router

1. Air carriers shall ensure that they are connected to the router. They shall ensure that their systems and infrastructure for the transfer of API data to the router pursuant to this Regulation are integrated with the router.

   Air carriers shall ensure that the connection to the router and the integration with it enables them to transfer the API data as well as to exchange any communications relating thereto, in a lawful, secure, effective and swift manner.

2. The Commission is empowered to adopt delegated acts in accordance with Article 19 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 12

Member States' costs

1. Costs incurred by the Member States in relation to their connections to and integration with the router referred to in Article 10 shall be borne by the general budget of the Union.

   However, the following costs shall be excluded and be borne by the Member States:

   (a) costs for project management, including costs for meetings, missions and offices;

   (b) costs for the hosting of national information technology (IT) systems, including costs for space, implementation, electricity and cooling;

   (c) costs for the operation of national IT systems, including operators and support contracts;

   (d) costs for the design, development, implementation, operation and maintenance of national communication networks.

2. Member States shall also bear the costs arising from the administration, use and maintenance of their connections to and integration with the router.

Article 13

Actions in case of technical impossibility to use the router

1. Where it is technically impossible to use the router to transmit API data because of a failure of the router, eu-LISA shall immediately notify the air carriers and PIUs of that technical impossibility in an automated manner. In that case, eu-LISA shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

   During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

2. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 10 of a Member State, the PIU of that Member State shall immediately notify the air carriers, the other PIUs, eu-LISA and the Commission of that technical impossibility in an automated manner. In that case, that Member State shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

   During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router.

Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

3. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 11 of an air carrier, that air carrier shall immediately notify the PIUs, eu-LISA and the Commission of that technical impossibility in an automated manner. In that case, that air carrier shall immediately take measures to address the technical impossibility to use the router and shall immediately notify those parties when it has been successfully addressed.

During the time period between those notifications, Article 4(6) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) shall not apply either to the API data in question during that time period.

When the technical impossibility has been successfully addressed, the air carrier concerned shall, without delay, submit to the competent national supervisory authority referred to in Article 15 a report containing all necessary details on the technical impossibility, including the reasons for the technical impossibility, its extent and consequences as well as the measures taken to address it.

Article 14

Liability regarding the router

If any failure of a Member State or an air carrier to comply with its obligations under this Regulation causes damage to the router, that Member State or air carrier shall be liable for such damage, unless and insofar as eu-LISA failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

CHAPTER 5

SUPERVISION, PENALTIES AND HANDBOOK

Article 15

National supervisory authority

1. Member States shall designate one or more national supervisory authorities responsible for monitoring the application within their territory by air carriers of the provisions of this Regulation and ensuring compliance with those provisions.

2. Member States shall ensure that the national supervisory authorities have all necessary means and all necessary investigative and enforcement powers to carry out their tasks under this Regulation, including by imposing the penalties referred to in Article 16 where appropriate. They shall 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 Union law.

3. Member States shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, notify the Commission of the name and the contact details of the authorities that they designated under paragraph 1 and of the detailed rules that they laid down pursuant to paragraph 2. They shall notify the Commission without delay of any subsequent changes or amendments thereto.

4. This Article is without prejudice to the powers of the supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680.

Article 16

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure they are implemented. The penalties provided for shall be effective, proportionate and dissuasive penalties.

Member States shall, by the date of application of this Regulation referred to in Article 21, second subparagraph, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.

Article 17

Practical handbook

The Commission shall, in close cooperation with the PIUs, other relevant Member States' authorities, the air carriers and relevant Union agencies, prepare and make publicly available a practical handbook, containing guidelines, recommendations and best practices for the implementation of this Regulation.

The practical handbook shall take into account the relevant existing handbooks.

The Commission shall adopt the practical handbook in the form of a recommendation.

CHAPTER 6

RELATIONSHIP TO OTHER EXISTING INSTRUMENTS

Article 18

Amendments to Regulation (EU) 2019/818

In Article 39, paragraphs 1 and 2 are replaced by the following:

"1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the SIS, Eurodac and ECRIS-TCN, in accordance with the respective legal instruments governing those systems, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes. The CRRS shall also support the objectives of Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*]."

* Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L …)"

"2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. eu-LISA shall also collect the data and statistics from the router referred to in Article 13(1) of Regulation (EU) …/… * [*this Regulation*]. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 74 of Regulation (EU) 2018/1862, Article 32 of Regulation (EU) 2019/816 and Article 13(1) of Regulation (EU) …/… * [*this Regulation*]."

CHAPTER 7

FINAL PROVISIONS

Article 19

Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 4(5) and (9), Article 5(3), Article 10(2) and Article 11(2) shall be conferred on the Commission for a period of five years from [*date of adoption of the Regulation*]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 4(5) and (9), Article 5(3), Article 10(2) and Article 11(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the

decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Article 20

Monitoring and evaluation

1. By [*four years after the date of entry into force of this Regulation*], and every four years thereafter, the Commission shall produce a report containing an overall evaluation of this Regulation, including an assessment of:

   (a) the application of this Regulation;

   (b) the extent to which this Regulation achieved its objectives;

   (c) the impact of this Regulation on the fundamental rights protected under Union law;

   (d) The Commission shall submit the evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Agency for Fundamental Rights. If appropriate, in light of the evaluation conducted, the Commission shall make a legislative proposal to the European Parliament and to the Council with a view to amending this Regulation.

2. The Member States and air carriers shall, upon request, provide the Commission with the information necessary to draft the report referred to in paragraph 1. However, Member States may refrain from providing such information if, and to the extent, necessary not to disclose confidential working methods or jeopardise ongoing investigations of their PIUs or other law enforcement authorities. The Commission shall ensure that any confidential information provided is appropriately protected.

Article 21

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from two years from the date at which the router starts operations, specified by the Commission in accordance with Article 27 of Regulation (EU) [API border management].

However, Article 4(5) and (9), Article 5(3), Article 10(2), Article 11(2) and Article 19 shall apply from [*Date of entry into force of this Regulation*].

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

The financial implications of this proposal are covered by the joint legislative financial statement annexed to the proposal for Regulation (EU) [API border management].