











Procedure file

Basic information	
<p>COD - Ordinary legislative procedure (ex-codecision procedure) Regulation</p> <p>2022/0425(COD)</p>	Awaiting Council's 1st reading position
<p>Collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime</p> <p>Amending Regulation 2019/818 2017/0352(COD)</p> <p>Subject</p> <p>2.20 Free movement of persons</p> <p>7.10 Free movement and integration of third-country nationals</p> <p>7.10.02 Schengen area, Schengen acquis</p> <p>7.10.04 External borders crossing and controls, visas</p> <p>7.30.20 Action to combat terrorism</p> <p>7.30.30 Action to combat crime</p> <p>Legislative priorities</p> <p>Joint Declaration 2022</p> <p>Joint Declaration 2023-24</p>	

Key players				
European Parliament	Committee responsible	Rapporteur	Appointed	
	<p>LIBE Civil Liberties, Justice and Home Affairs</p>	<p> KANKO Assita</p> <p>Shadow rapporteur</p> <p> LENAERS Jeroen</p> <p> TANG Paul</p> <p> OETJEN Jan-Christoph</p> <p> STRIK Tineke</p> <p> FEST Nicolaus</p> <p> DALY Clare</p>		28/03/2023
	Committee for opinion	Rapporteur for opinion	Appointed	
	<p>BUDG Budgets</p>	The committee decided not to give an opinion.		
	<p>TRAN Transport and Tourism</p>	<p> OETJEN Jan-Christoph</p>		22/02/2023

Key events

13/12/2022	Legislative proposal published	COM(2022)0731	Summary
13/02/2023	Committee referral announced in Parliament, 1st reading		
28/11/2023	Vote in committee, 1st reading		
28/11/2023	Committee decision to open interinstitutional negotiations with report adopted in committee		
07/12/2023	Committee report tabled for plenary, 1st reading	A9-0411/2023	Summary
11/12/2023	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
13/12/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
19/03/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	GEDA/A/(2024)001513	
24/04/2024	Debate in Parliament		
25/04/2024	Results of vote in Parliament		
25/04/2024	Decision by Parliament, 1st reading	T9-0377/2024	Summary

Technical information

Procedure reference	2022/0425(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
	Amending Regulation 2019/818 2017/0352(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 087-p2; Treaty on the Functioning of the EU TFEU 082-p2
Other legal basis	Rules of Procedure EP 165
Stage reached in procedure	Awaiting Council's 1st reading position
Committee dossier	LIBE/9/10977

Documentation gateway

Legislative proposal	COM(2022)0731	13/12/2022	EC	Summary
Document attached to the procedure	SWD(2022)0424	14/12/2022	EC	

Document attached to the procedure		N9-0017/2023 OJ C 084 07.03.2023, p. 0002	08/02/2023	EDPS	
Economic and Social Committee: opinion, report		CES0256/2023	27/04/2023	ESC	
Committee draft report		PE750.253	04/07/2023	EP	
Committee opinion	TRAN	PE746.973	19/07/2023	EP	
Amendments tabled in committee		PE752.818	05/09/2023	EP	
Committee report tabled for plenary, 1st reading/single reading		A9-0411/2023	07/12/2023	EP	Summary
Coreper letter confirming interinstitutional agreement		GEDA/A/(2024)001513	13/03/2024	CSL	
Text adopted by Parliament, 1st reading/single reading		T9-0377/2024	25/04/2024	EP	Summary
Commission response to text adopted in plenary		SP(2024)394	08/08/2024	EC	

Additional information

Research document	Briefing	15/04/2024
-------------------	--------------------------	------------

Collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

PURPOSE: to present new rules on the collection and transfer of advance passenger information (API) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

PROPOSED ACT: Regulation of the European Union and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: 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. 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.

In the EU, 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.

The joint processing of API and PNR data by competent law enforcement authorities substantially increases the effectiveness of the fight against serious crimes and terrorism in the EU. 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.

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.

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.

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.

CONTENT: the proposed Regulation 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. More specifically, it lays down rules on:

- the collection by air carriers of advance passenger information data (API data) on extra EU flights and selected intra EU flights;
- the transfer by air carriers to the router of the API data;

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

It will apply to air carriers conducting scheduled or non-scheduled extra-EU flights or intra-EU flights.

Overall, the proposal contains:

- 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;
- 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;
- 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;
- 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.

Budgetary implications

This proposal will have an impact on the budget and staff needs of eu-LISA and Member States competent border 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 in the proposed Regulation for the collection and transfer of API data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

For Member States, it is estimated that EUR 27 million (EUR 8 million under the current Multiannual Financial Framework) dedicated to upgrading the necessary national systems and infrastructures for border management authorities, and progressively up to EUR 5 million per year from 2028 onwards for the maintenance thereof, could be entitled for reimbursement by Border Management and Visa Instrument fund. 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.

Collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Assita KANKO (ECR, BE) on the 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 committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

API data to be collected by air carriers

The amended text stated that air carriers should collect API data of passengers, consisting of the passenger data and the flight information, respectively, on the flights for the purpose of transferring that API data to the router.

API data should include only the following passenger data for each passenger on the flight: (a) surname, given name(s); (b) date of birth, sex and nationality; (c) type and number of travel document and the three-letter code of the country that issued it; (d) expiry date of the validity of the travel document; (e) the Passenger Name Record number used by an air carrier to locate a passenger in its information system (PNR record locator); (f) the aircraft seat number allocated to a passenger; (g) the number and weight of checked baggage.

API data should include only the following flight information: the flight identification number(s); where applicable, the border crossing point of entry into the territory of the Member State; the airport code of entry into the territory of the Member State; the initial point of embarkation; the local date and estimated time of departure and arrival.

Collection of API data

Air carriers should collect the API data, using automated means to collect the machine-readable data of the travel document of the passenger concerned.

Where the use of automated means is not possible, air carriers should collect that data manually, either as part of the online check-in or as part of the check-in at the airport.

The collection of API data by automated means should be strictly limited to the alphanumeric data contained in the travel document and should not lead to the collection of any biometric data from it.

Storage and deletion of API data

Members suggested that air carriers should store, for a time period of 24 hours from the moment of departure of the flight, the API data relating to that passenger that they collected. They should immediately and permanently delete that API data after the expiry of that time period.

Air carriers or competent border authorities should immediately and permanently delete API data where they become aware that the API data collected was processed unlawfully or that the data transferred does not constitute API data.

Fundamental rights

The processing of API data and, in particular, API data constituting personal data, should remain strictly limited to what is necessary and

proportionate to achieve the objectives pursued by the Regulation. Furthermore, the processing of API data collected and transferred under the Regulation should not lead to any form of discrimination excluded by the Charter of Fundamental Rights of the European Union.

The Router

The report stated that in order to avoid that air carriers have to establish and maintain multiple connections with Passenger Information Units (PIUs) for the transfer of API data and PNR data, and to avoid the related inefficiencies and security risks, provision should be made for a single router, created and operated at the Union level, that should serve as a connection, filter and distribution point for those transfers.

In this regard, eu-LISA should design, develop, host and technically manage, a router for the purpose of facilitating the transfer of encrypted API and PNR data by the air carriers to the PIUs.

Methodology and criteria for the selection of intra-EU flights

Member States that decide to apply Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive) and consequently this Regulation to intra-EU flights should for the selection of those flights:

- carry out an objective, duly reasoned and non-discriminatory threat assessment;
- take into account only criteria which are relevant for the prevention, detection, investigation and prosecution of terrorist offences and serious crime having an objective link.

In situations of a genuine and present or foreseeable terrorist threat, Member States may apply Directive (EU) 2016/681 to all intra-EU flights arriving at or departing from its territory, in a decision that is limited in time to what is strictly necessary and that is open to effective review.

Logs

Members suggested that u-LISA should keep logs of all processing operations relating to the transfer of API data through the router under this Regulation.

Actions in the case of technical impossibility to use the router

eu-LISA should immediately notify air carriers and Passenger Information Units in an automated manner of the technical impossibility of using the router and take steps to remedy this technical impossibility.

Information to passengers

Air carriers should provide passengers with information on the purpose of the collection of their personal data, the type of personal data collected, the recipients of the personal data and the means to exercise the data subject rights. This information should be communicated to passengers in writing and in an easily accessible format at the moment of booking and at the moment of check-in, irrespective of the means used to collect the personal data at the moment of check-in.

Penalties

Member States should ensure that a systematic or persistent failure to comply with obligations set out in this Regulation is subject to financial penalties of up to 2% of an air carrier's global turnover of the preceding business year.

Collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

The European Parliament adopted by 438 votes to 35 abstentions, a legislative resolution on the 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 Parliaments position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

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 on extra EU flights and intra EU flights; (b) the transfer by air carriers to the router of the API data and other PNR data; (c) the transmission from the router to the Passenger Information Units (PIUs) of the API data and other PNR data on extra-EU flights and selected intra-EU flights.

This Regulation applies to air carriers conducting: (a) extra-EU flights; (b) intra-EU flights that will depart from, arrive in or make a stop-over on the territory of at least one Member State that notified its decision to apply Directive (EU) 2016/681 to intra-EU flights.

Collection and transfer of API data

Air carriers should collect API data of each passenger and crew member on flights to the EU to be transferred to the router. The API data should consist only of the following data relating to each passenger and crew member on the flight: the surname, the date of birth, sex and nationality; the type and number of the travel document and the three-letter code of the issuing country of the travel document; the number identifying a passenger name record used by an air carrier to locate a passenger within its information system (PNR record locator); seating and baggage information.

In addition, air carriers should collect certain flight information, such as the flight identification number, airport code, departure and arrival times and the air carrier's contact details.

Air carriers should collect the API data in such a manner that the API data that they transfer is accurate, complete and up-to-date. Compliance with this obligation does not require air carriers to check the travel document at the moment of boarding the aircraft, without prejudice to acts of national law that are compatible with Union law.

Where air carriers provide an online check-in process, they should enable passengers to provide API data by automated means during this online check-in process.

During a transitional period, air carriers should provide the possibility to passengers to provide API data manually as part of the online check-in.

Air carriers should transfer the API data: (a) for passengers: (i) per passenger at the moment of check-in, but not earlier than 48 hours prior to the scheduled departure time, and (ii) for all boarded passengers 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; (b) for all members of the crew immediately after flight closure, that is, once the crew is on board the aircraft in preparation for departure and it is no longer possible for them to leave the aircraft.

The storage period for API data is set at 48 hours. Where air carriers discover that the data they are storing has been unlawfully processed, or that the data does not constitute API data, they should delete it immediately and permanently.

The processing of API data collected and transferred under the Regulation must not lead to any form of discrimination prohibited by the Charter of Fundamental Rights of the European Union. Particular attention must be paid to children, the elderly, people with disabilities and vulnerable persons.

The router

The European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) should design, develop, host and technically manage a router to facilitate the transfer of encrypted API data by air carriers to the competent border authorities.

The router should verify, in an automated manner and on the basis of real-time air traffic data, whether the air carrier has transferred the API data. Each Member State should ensure that its Passenger Information Units, when receiving API and other PNR data, confirm to the router, immediately and in an automated manner, the receipt of such data.

Selection of intra-EU flights

Member States that decide to apply this Regulation to intra-EU flights should select such intra-EU flights. Member States may only apply Directive (EU) 2016/681 and consequently this Regulation to all intra-EU flights arriving at or departing from their territory in situations of a genuine and present or foreseeable terrorist threat, on the basis of a decision that is based on a threat assessment, limited in time to what is strictly necessary and open to effective review either by a court or by an independent administrative body whose decision is binding. In addition, selection must be based on an objective, duly reasoned and non-discriminatory assessment.

Data protection

The air carriers should be controllers, within the meaning of the GDPR, for the processing of API data constituting personal data in relation to their collection of that data and their transfer thereof to the router.

Air carriers should provide passengers, on flights covered by this Regulation, with information on the purpose of the collection of their personal data, the type of personal data collected, the recipients of the personal data and the means to exercise the data subject rights.

Governance

No later than the date of entry into force of the Regulation, the Management Board of eu-LISA should establish a Programme Management Board consisting of ten members. Technical matters related to the usage and functioning of the router should be discussed in the API-PNR Contact Group where eu-LISA representatives should be also present.

Sanctions

Member States should ensure that a recurrent failure to transfer API data is subject to proportionate financial penalties of up to 2% of the air carrier's global turnover for the previous financial year. Failure to comply with the other obligations set out in the Regulation should be subject to proportionate penalties, including financial penalties.

Transparency				
LENAERS Jeroen	Shadow rapporteur	LIBE	30/08/2023	International Air Transport Association KLM Royal Dutch Airlines
TANG Paul	Shadow rapporteur	LIBE	29/08/2023	Passenger Information Unit The Netherlands Koninklijke Marechaussee Douane
TANG Paul	Shadow rapporteur	LIBE	27/06/2023	DG HOME EDPS The International Air Transport Association (IATA)
OETJEN Jan-Christoph	Shadow rapporteur	LIBE	27/06/2023	IATA, EDPS
OETJEN Jan-Christoph	Rapporteur	LIBE	22/05/2023	Air France-KLM A4E Swiss

			LHG TUI Qatar Airways ERA Ryanair
--	--	--	---