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

2022/0425(COD) - 08/01/2025 - Final act

PURPOSE: to contribute to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

LEGISLATIVE ACT: Regulation (EU) 2025/13 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.

CONTENT: for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, this regulation lays down the rules on: (a) the **collection of advance passenger information** (API) by air carriers on extra-EU flights and intra-EU flights; (b) the transfer of API data and other PNR data by air carriers to the router; (c) the **transmission of API data and other PNR data** from the router to the passenger information units (PIUs) 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 the Commission of its decision to apply Directive (EU) 2016/681 to intra-EU flights.

Selection of intra-EU flights

Member States that decide to apply that Directive and consequently this Regulation to intra-EU flights will select such intra-EU flights. Member States may apply Directive (EU) 2016/681 and consequently this Regulation to all intra-EU flights arriving at or departing from their territory only 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. In other situations, a selective approach is provided for. Furthermore, the selection must be made on the basis of an objective, duly justified and non-discriminatory assessment.

Collection of data

The regulation sets out which API data air carriers must collect and transfer. API data consists of a **closed list of traveller information**, such as name, date of birth, nationality, travel document type, travel document number, seating information and baggage information. In addition, air carriers will be required to collect certain flight information, such as flight identification number, airport code and time of departure and arrival.

Air carriers will transfer API data:

- per passenger at the moment of check-in, but not earlier than 48 hours prior to the scheduled flight departure time; and for all boarded passengers immediately after flight closure;

- for all members of the crew immediately after flight closure.

Improving border controls and the fight against crime

The new regulation will allow law enforcement authorities to **combine travellers' API data with their Passenger Name Record (PNR)**. Passenger information, such as Passenger Name Record (PNR) and in particular Advance Passenger Information (API), is essential for identifying high-risk passengers, including those not otherwise known to law enforcement, for establishing links between members of criminal groups, and for countering terrorist activities.

Automated data collection

Air carriers will collect API data using automated means that allow the collection of machine-readable data from the passenger's travel document. Where the use of automated means is not technically possible, carriers may collect API data **manually, as an exception**, either during online check-in or during airport check-in.

Manual data entry during online check-in will in any case remain possible for a **transitional period** of two years. Verification mechanisms will be put in place by air carriers to ensure the accuracy of the data.

Protection of fundamental rights

Any processing of API data, and in particular API data constituting personal data, will be strictly limited to what is necessary and proportionate to achieve the objectives pursued by the regulation. Furthermore, the processing of any API data collected and transferred under the regulation should not lead to any form of discrimination precluded by the Charter.

Single router

A router, to be developed by eu-LISA, will receive the data collected by air carriers and will then transmit it to the relevant border management and law enforcement authorities. The router will check the data format and the data transfer. The measures to be taken in case of technical impossibility to use the router are specified.

Data protection responsibilities

Air carriers will be controllers 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. Each Member State will designate a competent authority as data controller. Air carriers will 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 their rights as data subjects.

Governance

By the date of entry into force of the Regulation, the eu-LISA Management Board will establish a Programme Management Board composed of ten members. Technical issues related to the use and operation of the router will be discussed in the **API-PNR Contact Group**, in which eu-LISA representatives should also be present.

Sanctions

Member States will 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 preceding financial year. Failure to

comply with other obligations set out in the regulation will be subject to proportionate penalties, including financial penalties.

ENTRY INTO FORCE: 28.1.2025. The regulation will apply in respect of API data from the date corresponding to two years from the date of entry into service of the router (four years for PNR data).