Official Journal
of the European Union

EN
L series

2025/12

8.1.2025

REGULATION (EU) 2025/12 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 19 December 2024

on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC

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 77(2), points (b) and (d), and Article 79(2), point (c), 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 ([1]),

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) The carrying out of border checks of persons at the external borders significantly contributes to ensuring the long-term security of the Union, its Member States and its citizens and, as such, remains an important safeguard, especially in the area without internal border control. Border checks are to be carried out in accordance with Regulation (EU) 2016/399 of the European Parliament and of the Council ([3]) where applicable, in order to help combat illegal immigration and prevent threats to the Member States' internal security, public policy, public health and international relations. Such border checks are to be carried out in such a way as to fully respect human dignity and be in full compliance with relevant Union law, including the Charter of Fundamental Rights of the European Union ('the Charter').

(2) The use of passenger data and flight information transferred ahead of the arrival of passengers, known as advance passenger information or API data, contributes to speeding up the required border checks during the border-crossing process. For the purposes of this Regulation that process concerns, more specifically, the crossing of borders between a third country or a Member State to which this Regulation does not apply and a Member State to which this Regulation applies. The use of API data strengthens border checks at those external borders by providing sufficient time to enable detailed and comprehensive border checks to be carried out on all passengers, without having a disproportionate negative effect on those travelling in good faith. Therefore, in the interest of the effectiveness and efficiency of border checks at external borders, an appropriate legal framework should be provided for to ensure that Member States' competent border authorities at such external border crossing points have access to API data prior to the arrival of passengers.

(3) The existing legal framework on API data, which consists of Council Directive 2004/82/EC ([4]) and national law transposing that Directive, has proven important in improving border checks, in particular by setting up a framework for Member States to introduce provisions for laying down obligations on air carriers to transfer API data on passengers transported into their territory. However, divergent practices remain at national level. In particular, API data are not systematically requested from air carriers and air carriers are faced with different requirements regarding the type of information to be collected and the conditions under which the API data need to be transferred to competent border authorities. Those divergences not only lead to unnecessary costs and complications for air carriers, but they are also prejudicial to ensuring effective and efficient pre-checks on persons arriving at external borders.

([1]) OJ C 228, 29.6.2023, p. 97.
([2]) Position of the European Parliament of 25 April 2024 (not yet published in the Official Journal) and decision of the Council of 12 December 2024.
([3]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).
([4]) 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).

(4) The existing legal framework needs to be updated and replaced to ensure that the rules regarding the collection and transfer of API data for the purpose of enhancing and facilitating the effectiveness and efficiency of border checks at external borders and for combating illegal immigration are clear, harmonised and effective, in accordance with the rules set out in Regulation (EU) 2016/399 for Member States to which it applies, and with national law where it does not apply.

(5) In order to ensure a consistent approach at both Union and international level as much as possible and in view of the rules on the collection of API data applicable at international level, the updated legal framework established by this Regulation should take into account the relevant practices internationally agreed with the air industry, such as in the context of the World Customs Organisation, International Aviation Transport Association and International Civil Aviation Organisation (ICAO) Guidelines on Advance Passenger Information.

(6) The collection and transfer of API data affect the privacy of individuals and entail the processing of their personal data. In order to fully respect their fundamental rights, in particular the right of respect for private life and the right to the protection of personal data, in accordance with the Charter, adequate limits and safeguards should be provided for. For example, any processing of API data and, in particular, API data constituting personal data should remain strictly limited to what is necessary for and proportionate to achieving the objectives pursued by this Regulation. In addition, it should be ensured that the processing of any API data collected and transferred under this Regulation does not lead to any form of discrimination precluded by the Charter.

(7) In order to achieve its objectives, this Regulation should apply to all air carriers conducting flights into the Union, as defined in this Regulation, irrespective of the place of establishment of the air carriers conducting those flights, and operating both scheduled and non-scheduled flights. The collection of data from any other civil aircraft operations, such as flight schools, medical flights, emergency flights, as well as from military flights, is not within the scope of this Regulation. This Regulation is without prejudice to the collection of data from such flights as provided for in national law that is compatible with Union law. The Commission should assess the feasibility of a Union scheme obliging operators of private flights to collect and transfer air passenger data.

(8) The obligations on air carriers to collect and transfer API data under this Regulation should include all passengers on flights into the Union, transit passengers whose final destination is outside of the Union and any off-duty crew member positioned on a flight by an air carrier in connection with their duties.

(9) In the interest of effectiveness and legal certainty, the items of information that together constitute the API data to be collected and subsequently transferred under this Regulation should be listed clearly and exhaustively, covering both information relating to each passenger and information on the flight taken by that passenger. Under this Regulation, and in accordance with international standards, such flight information should cover seating and baggage information, where such information is available, and information on the border crossing point of entry into the territory of the Member State concerned in all cases covered by this Regulation. Where baggage or seat information is available within other IT systems that the air carrier, its handler, its system provider or the airport authority has at its disposal, air carriers should integrate that information in the API data to be transferred to the competent border authorities. API data as defined and regulated under this Regulation do not include biometric data.

(10) In order to allow for flexibility and innovation, it should in principle be left to each air carrier to determine how it meets its obligations regarding the collection of API data set out in this Regulation, taking into account the different types of air carrier as defined in this Regulation and their respective business models, including as regards check-in times and cooperation with airports. However, considering that suitable technological solutions exist that allow certain API data to be collected automatically while ensuring that the API data concerned are accurate, complete and up to date, and having regard to the advantages of the use of such technology in terms of effectiveness and efficiency, air carriers should be required to collect such API data using automated means, by reading information from the machine-readable data of the travel document. Where the use of such automated means is not technically possible in exceptional circumstances, air carriers should exceptionally collect the API data manually, either as part of the online check-in process or as part of the check-in at the airport, in such a manner as to ensure compliance with their obligations under this Regulation.

(11) The collection of API data by automated means should be strictly limited to the alphanumerical data contained in the travel document and should not lead to the collection of any biometric data from it. As the collection of API data is part of the check-in process, either online or at the airport, this Regulation does not include an obligation for air carriers to check a travel document of the passenger at the moment of boarding. Compliance with this Regulation

does not include any obligation for passengers to carry a travel document at the moment of boarding. This should be without prejudice to obligations stemming from other Union legal acts or national law that is compatible with Union law.

(12) The collection of API data from travel documents should also be consistent with the ICAO standards on machine-readable travel documents, which have been incorporated into Union law by means of Regulation (EU) 2019/1157 of the European Parliament and of the Council ([5]), Council Regulation (EC) No 2252/2004 ([6]) and Council Directive (EU) 2019/997 ([7]).

(13) The requirements set out in this Regulation and the corresponding delegated and implementing acts should lead to the uniform implementation of this Regulation by the air carriers, thereby minimising the cost of the interconnection of their respective systems. To facilitate the harmonised implementation of those requirements by the air carriers, in particular as regards the data structure, format and transmission protocol, the Commission, on the basis of its cooperation with the competent border authorities, other Member States authorities, air carriers and relevant Union agencies, should ensure that the practical handbook to be prepared by the Commission provides all the necessary guidance and clarifications.

(14) In order to enhance the quality of API data, the router to be established under this Regulation should verify whether the API data transferred to it by air carriers comply with the supported data formats, including standardised data fields or codes, in terms of both content and structure. Where the verification determines that the data are not compliant with those data formats, the router should, immediately and in an automated manner, notify the air carrier concerned.

(15) It is important that the automated data collection systems and other processes established under this Regulation do not have a negative impact on the employees in the aviation industry, who are to be provided with upskilling and reskilling opportunities that would increase the efficiency and reliability of data collection and transfer as well as the working conditions in the sector.

(16) Passengers should have the possibility to provide certain API data themselves by automated means during an online check-in process, for example via a secure application on a passenger's smartphone, a computer or a webcam with the capability to read the machine-readable data of the travel document. Where passengers do not check in online, air carriers should provide them with the possibility to provide the required machine-readable API data during check-in at the airport with the assistance of a self-service kiosk or of air carriers' staff at the check-in counter. Without prejudice to air carriers' freedom to set air fares and define their commercial policy, it is important that the obligations under this Regulation do not lead to disproportionate obstacles for passengers unable to use online means to provide API data, such as additional fees for providing API data at the airport. In addition, this Regulation should provide for a transitional period during which passengers are given the possibility to provide API data manually as part of the online check-in process. In such cases, air carriers should use data verification techniques.

(17) With a view to ensuring the fulfilment of the rights provided for under the Charter, as well as ensuring accessible and inclusive travel options, especially for vulnerable groups and persons with disabilities, and in accordance with the rights of disabled persons and persons with reduced mobility when travelling by air set out in Regulation (EC) No 1107/2006 of the European Parliament and of the Council ([8]), air carriers, supported by the Member States, should ensure that an option for the provision of the necessary data by passengers at the airport is available at all times.

(18) In view of the advantages offered by using automated means for the collection of machine-readable API data and the clarity resulting from the technical requirements in that regard to be adopted under this Regulation, air carriers that decide to use automated means to collect the information that they are required to transmit under Directive 2004/82/EC should be provided with the possibility, but not the obligation, to apply those requirements, once

([5]) Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).

([6]) Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ L 385, 29.12.2004, p. 1).

([7]) Council Directive (EU) 2019/997 of 18 June 2019 establishing an EU Emergency Travel Document and repealing Decision 96/409/CFSP (OJ L 163, 20.6.2019, p. 1).

([8]) Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air (OJ L 204, 26.7.2006, p. 1).

adopted, in connection to such use of automated means, insofar as that Directive is applicable and permits it. Any such voluntary application of those specifications in application of Directive 2004/82/EC should not be understood as affecting in any way the obligations of air carriers and Member States under that Directive.

(19) With a view to ensuring that the pre-checks carried out in advance by competent border authorities are effective and efficient, the API data transferred to those authorities should contain the data of passengers that are effectively set to cross the external borders, that is, of passengers that are effectively on board of the aircraft, irrespective of whether the final destination of the passenger is inside or outside the Union. Therefore, air carriers should transfer API data immediately after flight closure. Moreover, API data help the competent border authorities to distinguish legitimate passengers from passengers who might be of interest and therefore require additional verifications, which would necessitate further coordination and preparation of follow-up measures to be taken upon arrival. That could occur, for example, in cases of an unexpected number of passengers of interest, whose physical checks at the borders could adversely affect the border checks and waiting times at the borders of other legitimate passengers. To provide the competent border authorities with an opportunity to prepare adequate and proportionate measures at the border, such as temporarily reinforcing or redeploying staff, particularly for flights where the time between the flight closure and the arrival at the external borders is insufficient to allow the competent border authorities to prepare the most appropriate response, API data should also be transferred prior to boarding, at the moment of check-in of each passenger.

(20) In order to avoid any risk of misuse and in line with the principle of purpose limitation, the competent border authorities should be expressly precluded from processing the API data that they receive under this Regulation for any purpose other than those explicitly provided for in this Regulation and in accordance with the rules set out in Regulation (EU) 2016/399 for Member States to which that Regulation applies or, where that Regulation does not apply, in accordance with the relevant rules set out in national law.

(21) To ensure that competent border authorities have sufficient time to carry out pre-checks effectively on all passengers, including passengers on long-haul flights and those travelling on connecting flights, as well as sufficient time to ensure that the API data collected and transferred by air carriers are accurate, complete and up to date, and where necessary to request additional clarifications, corrections or completions from air carriers, in order to ensure that API data remain available until all passengers have effectively presented themselves at the border crossing point, the competent border authorities should store the API data that they received under this Regulation for a fixed period of time that remains limited to what is strictly necessary for those purposes. In exceptional circumstances where individual passengers, after landing, do not present themselves at a border crossing point within such fixed period of time, the Member States should have the possibility to enable their competent border authorities to store the API data of such individual passengers until they present themselves at a border crossing point or at the latest for an additional fixed period of time. Where Member States want to make use of such possibility, Member States should be responsible to put in place the appropriate means to identify such individual passengers, in order to ensure that the longer retention of their specific API data remain limited to what is strictly necessary.

(22) In order to be able to respond to requests for additional clarifications, corrections or completions by the competent border authorities, air carriers should store the API data that they transferred under this Regulation for a fixed and strictly necessary period of time. Beyond that, and with a view to enhancing the travel experience of legitimate passengers, air carriers should be able to retain and use the API data where necessary for the normal course of their business in particular for travel facilitation, in compliance with the applicable law and in particular Regulation (EU) 2016/679 of the European Parliament and of the Council ([9]).

(23) In order to avoid a situation in which air carriers have to establish and maintain multiple connections with the competent border authorities of the Member States for the transfer of API data collected under this Regulation, and thereby avoid the related inefficiencies and security risks, provision should be made for a single router, created and operated at Union level in accordance with this Regulation and Regulation (EU) 2025/13 of the European Parliament and of the Council ([10]), that serves as a connection and distribution point for those transfers. In the interest of efficiency and cost-effectiveness, the router should, to the extent technically possible and in full compliance with the

([9]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([10]) Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 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 (OJ L, 2025/13, 8.1.2025, ELI: http://data.europa.eu/eli/reg/2025/13/oj).

rules of this Regulation and Regulation (EU) 2025/13 rely on technical components from other relevant systems created under Union law, in particular the web service referred to in Regulation (EU) 2017/2226 of the European Parliament and of the Council ([11]), the carrier gateway referred to in Regulation (EU) 2018/1240 of the European Parliament and of the Council ([12]) and the carrier gateway referred to in Regulation (EC) No 767/2008 of the European Parliament and of the Council ([13]). In order to reduce the impact on air carriers and ensure a harmonised approach towards air carriers, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), established by Regulation (EU) 2018/1726 of the European Parliament and of the Council ([14]), should design the router, to the extent technically and operationally possible, in a way that is coherent and consistent with the obligations for air carriers set out in Regulations (EC) No 767/2008, (EU) 2017/2226 and (EU) 2018/1240.

(24) In order to improve the efficiency of the transmission of air traffic data and support the monitoring of the API data transmitted to competent border authorities, the router should receive real-time flight traffic data collected by other organisations, such as the European Organisation for the Safety of Air Navigation (Eurocontrol).

(25) Under this Regulation, the router should transmit the API data, in an automated manner, to the relevant competent border authorities, which should be determined on the basis of the border crossing point of entry into the territory of the Member State included in the API data in question. In order to facilitate the distribution process, each Member State should indicate which border authorities are competent to receive the API data transmitted from the router. It is possible for Member States to establish a single data entry point that receives the API data from the router and that immediately and in an automated manner forwards those data to the competent border authorities of the Member State concerned. To ensure the proper functioning of this Regulation and in the interest of transparency, the information on the competent border authorities should be made public.

(26) The router should serve only to facilitate the transfer of API data from the air carriers to the competent border authorities in accordance with this Regulation, and should not be a repository of API data. Therefore, and in order to minimise any risk of unauthorised access or other misuse and in accordance with the principle of data minimisation, no storage should take place unless strictly necessary for technical purposes related to the transmission and the API data should be deleted from the router, immediately, permanently and in an automated manner, from the moment that the transmission has been completed.

(27) In order to allow air carriers to benefit as soon as possible from the advantages offered by the use of the router developed by eu-LISA in accordance with this Regulation and Regulation (EU) 2025/13, and to gain experience in using it, air carriers should be provided with the possibility, but not the obligation, to use the router to transfer the information that they are required to transfer under Directive 2004/82/EC during an interim period. That interim period should commence at the moment at which the router starts operations and end when the obligations under that Directive cease to apply. With a view to ensuring that any such voluntary use of the router takes place in a responsible manner, the prior written agreement of the Member State that is to receive the information should be required, upon request of the air carrier and after that Member State having conducted verifications and obtained assurances, as necessary. Similarly, in order to avoid a situation in which air carriers repeatedly start and stop using the router, once an air carrier starts such use on a voluntary basis, it should be required to continue it, unless there are objective reasons to discontinue the use of the router for the transfer of the information to the responsible authorities of the Member State concerned, such as it having become apparent that the information is not transferred in a lawful, secure, effective and swift manner. In the interest of the proper application of the possibility

([11]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

([12]) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

([13]) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas and residence permits (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

([14]) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

of voluntarily using the router, with due regard to the rights and interests of all affected parties, the necessary rules on consultations and the provision of information should be provided for in this Regulation. Any such voluntary use of the router in application of Directive 2004/82/EC as provided for in this Regulation should not be understood as affecting in any way the obligations of air carriers and Member States under that Directive.

(28) The router to be created and operated under this Regulation and Regulation (EU) 2025/13 should reduce and simplify the technical connections needed to transfer API data under this Regulation, limiting them to a single connection per air carrier and per competent border authority. Therefore, this Regulation should provide for the obligation for the competent border authorities and air carriers to each establish such a connection to, and achieve the required integration with, the router, to ensure that the system for transferring API data established by this Regulation can function properly. The design and development of the router by eu-LISA should enable the effective and efficient connection and integration of air carriers' systems and infrastructure by providing for all relevant standards and technical requirements. To ensure the proper functioning of the system set up by this Regulation, detailed rules should be provided for. When designing and developing the router, eu-LISA should ensure that API data transferred by air carriers and transmitted to competent border authorities are encrypted in transit.

(29) In view of the Union interests at stake, all the costs incurred by eu-LISA for the performance of its tasks under this Regulation in respect of the router should be borne by the Union budget, including the design and development of the router, the hosting and technical management of the router, and the governance structure at eu-LISA to support the design, development, hosting and technical management of the router. The same might apply for the costs incurred by the Member States in relation to their connections to, and integration with, the router and their maintenance, as required under this Regulation, in accordance with the applicable Union law. It is important that the Union budget provides appropriate financial support to the Member States for those costs. To that end, the financial needs of the Member States should be supported by the general budget of the Union, in accordance with the eligibility rules and co-financing rates set by the relevant Union legal acts. The annual Union contribution allocated to eu-LISA should cover the needs related to the hosting and the technical management of the router based on an assessment carried out by eu-LISA. The Union budget should also cover the support, such as training, provided by eu-LISA to air carriers and competent border authorities to enable effective transfer and transmission of API data through the router. The costs incurred by the independent national supervisory authorities in relation to the tasks entrusted to them under this Regulation should be borne by the respective Member States.

(30) It cannot be excluded that, due to exceptional circumstances and despite all reasonable measures having been taken in accordance with this Regulation, the central infrastructure or one of the technical components of the router, or the communication infrastructures connecting the competent border authorities and the air carriers thereto, fail to function properly, thus leading to a technical impossibility for air carriers to transfer, or for competent border authorities to receive, 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 such API data to the router should cease to apply for as long as the technical impossibility persists. However, to ensure the availability of API data necessary for enhancing and facilitating the effectiveness and efficiency of border checks at the external borders and combatting illegal immigration, air carriers should continue to collect and store API data so that they can be transferred as soon as the technical impossibility has been resolved. In order to minimise the duration and negative consequences of any technical impossibility, the parties concerned should in such a case immediately inform each other and immediately take all measures necessary 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 to the fact that air carriers are subject to penalties if they fail to meet those obligations, including in cases where 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.

(31) Where air carriers maintain direct connections to competent border authorities for the transfer of API data, those connections can constitute appropriate means, ensuring the necessary level of data security, to transfer API data directly to the competent border authorities where it is technically impossible to use the router. Competent border authorities should be able, in the exceptional case of technical impossibility to use the router, to request air carriers to use such appropriate means, which does not imply an obligation on air carriers to maintain or introduce such direct connections or any other appropriate means, ensuring the necessary level of data security, to transfer API data directly to the competent border authorities. The exceptional transfer of API data by any other appropriate means, such as encrypted email or a secure web portal, and excluding the use of non-standard electronic formats, should

ensure the necessary level of data security, data quality and data protection. API data received by the competent border authorities by such other appropriate means should be further processed in accordance with the rules and data protection safeguards set out in Regulation (EU) 2016/399 and applicable national law. Following the notification from eu-LISA that the technical impossibility has been successfully addressed, and where it is confirmed that the transmission of the API data through the router to the competent border authority has been completed, the competent border authority should immediately delete the API data they previously received by any other appropriate means. That deletion should not affect specific cases where the API data that competent border authorities received by any other appropriate means has meanwhile been further processed in accordance with Regulation (EU) 2016/679 for the specific purposes of enhancing and facilitating the effectiveness and efficiency of border checks at external borders and of combating illegal immigration.

(32) In the interest of ensuring compliance with the fundamental right to protection of personal data, this Regulation should identify the controller and processor and set out rules on audits. 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 in line with the generally applicable Union legal acts on the protection of personal data, in particular Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council ([15]).

(33) Without prejudice to more specific rules laid down in this Regulation for the processing of personal data, Regulation (EU) 2016/679 should apply to the processing of personal data by the Member States and air carriers under this Regulation. Regulation (EU) 2018/1725 should apply to the processing of personal data by eu-LISA when carrying out its responsibilities under this Regulation.

(34) Taking into account the right of passengers to be informed of the processing of their personal data, Member States should ensure that passengers are provided with accurate information about the collection of API data, the transfer of such data to the competent border authorities and their rights as data subjects that is easily accessible and easy to understand, at the moment of booking and at the moment of check-in.

(35) The personal data protection audits that Member States are responsible for should be carried out by the independent supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 or by an auditing body entrusted with this task by the supervisory authority.

(36) The purposes of the processing operations under this Regulation, namely the transmission of API data from air carriers via the router to the competent border authorities of the Member States, are to assist those authorities in the performance of their border management obligations and tasks related to combating illegal immigration. Therefore, Member States should designate authorities to be controllers for the processing of the data in the router, the transmission of the data from the router to the competent border authorities, and the subsequent processing of those data to enhance and facilitate border checks at external borders. Member States should communicate those authorities to the Commission and eu-LISA. For the processing of personal data in the router, Member States should be joint controllers in accordance with Article 26 of Regulation (EU) 2016/679. The air carriers, in turn, should be separate controllers with regard to the processing of API data constituting personal data under this Regulation. On this basis, both the air carriers and the competent border authorities should be separate controllers with regard to the processing operations for API data under this Regulation. As eu-LISA is responsible for the design, development, hosting and technical management of the router, it should be the processor for the processing of API data constituting personal data via the router, including the transmission of the data from the router to the competent border authorities and the storage of those data on the router insofar as such storage is needed for technical purposes.

(37) 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 as national API supervision authorities charged with monitoring the application of those rules. Member States can designate their competent border authorities as national API supervision authorities. The rules of this Regulation on such monitoring, including as regards the

([15]) 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).

imposition of penalties where necessary, should leave the tasks and powers of the supervisory authorities established in accordance with Regulation (EU) 2016/679 unaffected, including in relation to the processing of personal data under this Regulation.

(38) Effective, proportionate and dissuasive penalties, which include financial as well as non-financial penalties, should be provided for by Member States against those air carriers failing to meet their obligations under this Regulation, including on the collection of API data by automated means and the transfer of the data in accordance with the required time frames, formats and protocols. In particular, Member States should ensure that a recurrent failure on the part of air carriers as legal persons to comply with their obligation to transfer any API data to the router in accordance with this Regulation is subject to proportionate financial penalties of up to 2 % of the air carrier's global turnover of the preceding financial year. In addition, Member States should be able to apply penalties, including financial penalties, to air carriers for other forms of non-compliance with obligations under this Regulation.

(39) When providing for rules on the penalties applicable to air carriers under this Regulation, Member States could take into account the technical and operational feasibility of ensuring complete data accuracy. Additionally, when penalties are imposed, their application and value should be established. National API supervision authorities could take into consideration the actions undertaken by the air carrier to mitigate the issue as well as its level of cooperation with national authorities.

(40) There should be a single governance structure for the purposes of this Regulation and Regulation (EU) 2025/13. With the objective of enabling and fostering communication between the representatives of air carriers and the representatives of Member States authorities competent under this Regulation and under Regulation (EU) 2025/13 to have API data transmitted from the router, two dedicated bodies should be established at the latest two years after the start of operations of the router. 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. Policy matters, such as in relation to penalties, should be discussed in the API Expert Group.

(41) As this Regulation provides for the establishment of new rules on the collection and transfer of API data for the purpose of enhancing and facilitating the effectiveness and efficiency of border checks at external borders, Directive 2004/82/EC should be repealed.

(42) As the router should be designed, developed, hosted and technically managed by eu-LISA, it is necessary to amend Regulation (EU) 2018/1726 by adding that task to the tasks of eu-LISA. In order to store reports and statistics of the router on the central repository for reporting and statistics (CRRS) established by Regulation (EU) 2019/817 of the European Parliament and of the Council [16], it is necessary to amend that Regulation. In order to support the enforcement of this Regulation by the national API supervision authority, it is necessary that the amendments to Regulation (EU) 2019/817 include provisions on statistics on whether the API data are accurate and complete, for example by indicating whether the data were collected by automated means. It is also important to collect reliable and useful statistics concerning the implementation of this Regulation in order to support its objectives and inform the evaluations under this Regulation. Such statistics should not contain any personal data. Therefore, the CRRS should provide statistics based on API data only for the implementation and effective monitoring of the application of this Regulation. The data that the router automatically transmits to the CRRS to that end should not allow for the identification of the passengers concerned.

(43) In order to increase clarity and legal certainty, to contribute to ensuring data quality, ensuring the responsible use of the automated means for the collection of machine-readable API data under this Regulation and ensuring the manual collection of API data in exceptional circumstances and during the transitional period, to provide clarity on the technical requirements that are applicable to air carriers and that are needed to ensure the API data that they collected under this Regulation are transferred to the router in a secure, effective and swift manner, and to ensure that inaccurate or incomplete data or data that are no longer up to date are corrected, completed or updated, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission to terminate the transitional period for the manual collection of API data; to adopt measures relating to the technical requirements and operational rules with which air carriers should comply with regard to the use of automated means for the collection of machine-readable API data under this Regulation, for the manual collection of API data in exceptional circumstances, and for the collection of API data during the

[16] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

transitional period, including on requirements for data security; to lay down detailed rules on the common protocols and supported data formats to be used for the encrypted transfer of API data by air carriers, including requirements for data security; and to lay down rules on correcting, completing and updating API data. It is of particular importance that the Commission carry out appropriate consultations with relevant stakeholders, including air carriers, 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 of 13 April 2016 on Better Law-Making ([17]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Taking into account the state of the art, those technical requirements and operational rules might change over time.

(44) In order to ensure uniform conditions for the implementation of this Regulation, namely as regards the start of operations of the router; the technical and procedural rules for the data verifications and notifications; the technical and procedural rules for the transmission of API data from the router to the competent border authorities in a way that ensures that the transmission is secure, effective and swift and impacts passengers' travel and air carriers no more than necessary, and the competent border authorities' and air carriers' connections to and integration with the router, and to specify the responsibilities of the Member States as joint controllers, such as regards the identification and management of security incidents, including of personal data breaches, and the relationship between the joint controllers and eu-LISA as the processor, including the assistance of eu-LISA to the controllers with appropriate technical and organisational measures, insofar as it is possible, for the fulfilment of the controller's obligations to respond to requests for exercising the data subject's rights, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([18]).

(45) All interested parties, and in particular the air carriers and the competent border authorities, should be afforded sufficient time to make the preparations necessary 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 be finalised only 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 on which the router starts operations, as specified by the Commission in accordance with this Regulation and Regulation (EU) 2025/13. However, it should be possible for the Commission to adopt delegated and implementing 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.

(46) The design and development phases of the router established under this Regulation and Regulation (EU) 2025/13 should be commenced and completed as soon as possible so that the router can start operations as soon as possible, which also requires the adoption of the relevant delegated and implementing acts provided for by this Regulation. For the smooth and effective development of those phases, a dedicated Programme Management Board should be established with the function to supervise eu-LISA on fulfilling its tasks during those phases. It should cease to exist two years after the router has started its operations. In addition, a dedicated advisory body, the API-PNR Advisory Group, should be created in accordance with Regulation (EU) 2018/1726, with the objective of providing expertise to eu-LISA and to the Programme Management Board on the design and development phases of the router, as well as to eu-LISA on the hosting and management of the router. The Programme Management Board and the API-PNR Advisory Group should be established and operated following the models of existing programme management boards and advisory groups.

(47) This Regulation should be subject to regular evaluations to ensure the monitoring of its effective application. In particular, the collection of API data should not be to the detriment of the travel experience of legitimate passengers. Therefore, the Commission should include in its regular evaluation reports on the application of this Regulation an assessment of the impact of this Regulation on the travel experience of legitimate passengers. The evaluation should also include an assessment of the quality of the data sent by the router, as well as the performance of the router in respect of the competent border authorities.

([17]) OJ L 123, 12.5.2016, p. 1.
([18]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(48) The clarification provided by this Regulation regarding the application of specifications concerning the use of automated means in application of Directive 2004/82/EC should also be provided without delay. Therefore, the provisions on those matters should apply from the date of the entry into force of this Regulation. In addition, in order to allow for the voluntary use of the router as soon as possible, the provisions on such use, as well as certain other provisions needed to ensure that such use takes place in a responsible manner, should apply from the earliest possible moment, that is, from the moment at which the router starts operations.

(49) Given that this Regulation requires additional adjustment and administrative costs by air carriers, the overall regulatory burden for the aviation sector should be kept under close review. Against this backdrop, the report evaluating the functioning of this Regulation should assess the extent to which the objectives of this Regulation have been met and the extent to which it has had an impact on the competitiveness of the sector.

(50) This Regulation is without prejudice to the competences of Member States with regard to national law concerning national security, provided that such law complies with Union law.

(51) This Regulation is without prejudice to the competence of Member States to collect, under their national law, passenger data from transportation providers other than those specified in this Regulation, provided that such national law complies with Union law.

(52) Since the objectives of this Regulation, namely enhancing and facilitating the effectiveness and efficiency of border checks at external borders and combating illegal immigration, relate to matters that are inherently of a cross-border nature, they 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 European Union (TEU). 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 those objectives.

(53) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(54) Ireland is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC ([19]).

(55) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis* ([20]), which fall within the area referred to in Article 1, point A, of Council Decision 1999/437/EC ([21]).

(56) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([22]), which fall within the area referred to in Article 1, point A, of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/146/EC ([23]).

(57) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association

([19]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).
([20]) OJ L 176, 10.7.1999, p. 36.
([21]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).
([22]) OJ L 53, 27.2.2008, p. 52.
([23]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).

with the implementation, application and development of the Schengen *acquis* ([24]) which fall within the area referred to in Article 1, point A, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([25]).

(58) As regards Cyprus, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 3(1) of the 2003 Act of Accession.

(59) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 8 February 2023 ([26]),

HAVE ADOPTED THIS REGULATION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

For the purpose of enhancing and facilitating the effectiveness and efficiency of border checks at external borders and of combating illegal immigration, this Regulation lays down rules on:

(a) the collection of advance passenger information (API) by air carriers;

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

(c) the transmission of API data from the router to the competent border authorities.

This Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725.

Article 2

Scope

This Regulation applies to air carriers conducting flights into the Union.

Article 3

Definitions

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

(1) 'air carrier' means an air carrier as defined in Article 3, point (1), of Directive (EU) 2016/681 of the European Parliament and of the Council ([27]);

(2) 'border checks' means border checks as defined in Article 2, point 11, of Regulation (EU) 2016/399;

([24]) OJ L 160, 18.6.2011, p. 21.
([25]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).
([26]) OJ C 84, 7.3.2023, p. 2.
([27]) 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).

(3) ‘flights into the Union’ means flights flying from the territory either of a third country or of a Member State to which this Regulation does not apply, and planned to land on the territory of a Member State or Member States to which this Regulation applies;

(4) ‘border crossing point’ means a border crossing point as defined in Article 2, point 8, of Regulation (EU) 2016/399;

(5) ‘scheduled flight’ means a flight that operates according to a fixed timetable, for which tickets can be purchased by the general public;

(6) ‘non-scheduled flight’ means a flight that does not operate according to a fixed timetable and that is not necessarily part of a regular or scheduled route;

(7) ‘competent border authority’ means the authority that is empowered by a Member State to carry out border checks and that is designated and notified by that Member State in accordance with Article 14(2);

(8) ‘passenger’ means any person, excluding on-duty members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person’s registration in the passenger list;

(9) ‘advance passenger information’ or ‘API data’ means the passenger data and the flight information referred to in Article 4(2) and (3) respectively;

(10) ‘the router’ means the router referred to in Article 11 of this Regulation and Article 9 of Regulation (EU) 2025/13;

(11) ‘personal data’ means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(12) ‘real-time flight traffic data’ means information on the inbound and outbound flight traffic of an airport covered by this Regulation.

CHAPTER 2

COLLECTION, TRANSFER, STORAGE AND DELETION OF API DATA

Article 4

Collection of API data by air carriers

1. Air carriers shall collect the API data of each passenger on flights into the Union to be transferred to the router in accordance with Article 6. Where the flight is code-shared between air carriers, the obligation to transfer the API data shall be on the air carrier that operates the flight.

2. The API data shall consist only of the following data relating to each passenger on the flight:

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

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

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

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

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

(f) the seating information corresponding to the seat in the aircraft assigned to a passenger, where such information is available;

(g) the baggage tag number or numbers and the number and weight of checked bags, where such information is available;

(h) a code indicating the method used to capture and validate the data referred to in points (a) to (d).

3. The API data shall also consist only of the following flight information relating to the flight of each passenger:

(a) the flight identification number or, where the flight is code-shared between air carriers, the flight identification numbers, or, if no such number exists, other clear and suitable means to identify the flight;

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

(c) the code of the airport of arrival or, where the flight is planned to land in one or several airports within the territories of one or more Member States to which this Regulation applies, the codes of the airports of call on the territories of the Member States concerned;

(d) the code of the airport of departure of the flight;

(e) the code of the airport of the initial point of embarkation, where available;

(f) the local date and time of departure;

(g) the local date and time of arrival;

(h) the contact details of the air carrier;

(i) the format used for the transfer of API data.

Article 5

Means of collecting API data

1. Air carriers shall collect the API data pursuant to Article 4 in a manner that ensures that the API data that they transfer in accordance with Article 6 are accurate, complete and up to date.

2. Air carriers shall collect the API data referred to in Article 4(2), points (a) to (d), using automated means to collect the machine-readable data of the travel document of the passenger concerned. They shall do so in accordance with the detailed technical requirements and operational rules referred to in paragraph 7 of this Article, once such rules have been adopted and are applicable.

Where air carriers provide an online check-in process, they shall enable passengers to provide the API data referred to in Article 4(2), points (a) to (d), by automated means during that online check-in process. For passengers that do not check in online, air carriers shall enable those passengers to provide those API data by automated means during check-in at the airport with the assistance of a self-service kiosk or of air carriers' staff at the counter.

Where the use of automated means is not technically possible, air carriers shall exceptionally collect the API data referred to in Article 4(2), points (a) to (d), manually, either as part of the online check-in or as part of the check-in at the airport, in such a manner as to ensure compliance with paragraph 1 of this Article.

3. Any automated means used by air carriers to collect API data under this Regulation shall be reliable, secure and up to date. Air carriers shall ensure that API data are encrypted during the transfer of such data from the passenger to the air carrier.

4. During a transitional period, and in addition to the automated means referred to in paragraph 3, air carriers shall make it possible for passengers to provide API data manually as part of the online check-in. In such cases, air carriers shall use data verification techniques to ensure compliance with paragraph 1.

5. The transitional period referred to in paragraph 4 shall not affect the right of air carriers to verify, at the airport prior to the boarding of the aircraft, API data collected as part of the online check-in in order to ensure compliance with paragraph 1, in accordance with the applicable Union law.

6. The Commission is empowered to adopt, as of the date four years after the start of operations of the router referred to in Article 34, and on the basis of an evaluation of the availability and accessibility of automated means to collect API data, a delegated act in accordance with Article 44 to terminate the transitional period referred to in paragraph 4 of this Article.

7. The Commission is empowered to adopt delegated acts in accordance with Article 44 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), using automated means in accordance with paragraphs 2 and 3 of this Article, and for the manual collection of API data in exceptional circumstances in accordance with paragraph 2 of this Article and during the transitional period referred to in paragraph 4 of this Article. Those technical requirements and operational rules shall include requirements for data security and for using the most reliable automated means available to collect the machine-readable data of a travel document.

8. Air carriers that use automated means to collect the information referred to in Article 3(1) and (2) of Directive 2004/82/EC shall be entitled to do so applying the technical requirements relating to such use referred to in paragraph 7 of this Article, in accordance with that Directive.

Article 6

Obligations for air carriers regarding transfers of API data

1. Air carriers shall transfer the encrypted API data to the router by electronic means for the purposes of their transmission to the competent border authorities in accordance with Article 14. Air carriers shall transfer the API data in accordance with the detailed rules referred to in paragraph 3 of this Article, once such rules have been adopted and are applicable.

2. Air carriers shall transfer the API data:

(a) per passenger at the moment of check-in, but not earlier than 48 hours prior to the scheduled flight departure time; and

(b) for all boarded passengers immediately after flight closure, namely once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or to leave the aircraft.

3. The Commission is empowered to adopt delegated acts in accordance with Article 44 to supplement this Regulation by laying down the necessary detailed rules on the common protocols and supported data formats to be used for the encrypted transfers of API data to the router referred to in paragraph 1 of this Article, including the transfer of API data at the moment of check-in and requirements for data security. Such detailed rules shall ensure that air carriers transfer API data using the same structure and content.

Article 7

Processing of API data by competent border authorities

The competent border authorities shall process API data that they receive in accordance with this Regulation solely for the purpose of enhancing and facilitating the effectiveness and efficiency of border checks at external borders and of combating illegal immigration.

The competent border authorities shall not process API data in such a way as to result in the profiling of individuals as referred to in Article 22 of Regulation (EU) 2016/679 or to discriminate against persons on the grounds listed in Article 21 of the Charter.

Article 8

Storage period and deletion of API data

1. Air carriers shall store, for a period of 48 hours from the moment of receipt by the router of the API data transferred to it in accordance with Article 6(2), points (a) and (b), the API data that they collected pursuant to Article 4. They shall immediately and permanently delete such API data after the expiry of that period, 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 applicable law, and to Article 16(1) and (3).

2. The competent border authorities shall store, for a period of 48 hours from the moment of their receipt, the API data transmitted to them pursuant to Article 14 following the transfer pursuant to Article 6(2), points (a) and (b). They shall immediately and permanently delete such API data after the expiry of that period.

In exceptional cases, the competent border authorities may retain API data for an additional period of up to 48 hours only insofar as such API data refer to passengers who did not present themselves at a border crossing point during the period referred to in the first subparagraph.

Article 9

Correcting, completing and updating API data

1. Where an air carrier becomes aware that data that it stores under this Regulation were processed unlawfully, or do not constitute API data, it shall immediately and permanently delete those data. If those data have been transferred to the router, the air carrier 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 competent border authority that received the data transmitted through the router. That competent border authority shall immediately and permanently delete those data.

2. Where an air carrier becomes aware that the data that it stores under this Regulation are inaccurate, incomplete or no longer up to date, it shall immediately correct, complete or update those data. This is without prejudice to the possibility for air carriers to retain and use the data where necessary for the normal course of their business in compliance with the applicable law.

3. Where an air carrier becomes aware after the transfer of API data under Article 6(2), point (a), but before the transfer under Article 6(2), point (b), that the data it has transferred are inaccurate, the air carrier shall immediately transfer the corrected API data to the router.

4. Where an air carrier becomes aware, after the transfer of API data under Article 6(2), point (a) or (b), that the data it has transferred are inaccurate, incomplete or no longer up to date, the air carrier shall immediately transfer the corrected, completed or updated API data to the router.

5. Where a competent border authority becomes aware, after the transmission of API data under Article 14, that the data are inaccurate, incomplete or no longer up to date, it shall immediately delete those data, unless those data are required to ensure compliance with the obligations laid down in this Regulation.

6. The Commission is empowered to adopt delegated acts in accordance with Article 44 to supplement this Regulation by laying down the necessary detailed rules on correcting, completing and updating API data within the meaning of this Article.

Article 10

Fundamental rights

1. The collection and processing of personal data in accordance with this Regulation and Regulation (EU) 2025/13 by air carriers and competent authorities shall not result in the discrimination against persons on the grounds listed in Article 21 of the Charter of Fundamental Rights of the European Union (the 'Charter').

2. This Regulation shall fully respect human dignity and the fundamental rights and principles recognised by the Charter, including the right to respect for one's private life, to asylum, to the protection of personal data, to freedom of movement and to effective legal remedies.

3. Particular attention shall be paid to children, the elderly, persons with a disability and vulnerable persons. The best interests of the child shall be a primary consideration when implementing this Regulation.

CHAPTER 3

PROVISIONS RELATING TO THE ROUTER

Article 11

The router

1. eu-LISA shall design, develop, host and technically manage, in accordance with Articles 25 and 26, a router for the purpose of facilitating the transfer of encrypted API data by air carriers to the competent border authorities in accordance with this Regulation.

2. The router shall be composed of:

(a) a central infrastructure, including a set of technical components enabling the reception and transmission of encrypted API data;

(b) a secure communication channel between the central infrastructure and the competent border authorities, and a secure communication channel between the central infrastructure and the air carriers, for the transfer and transmission of API data and for any communications relating thereto;

(c) a secure channel to receive real-time flight traffic data.

3. Without prejudice to Article 12 of this Regulation, the router shall, where appropriate and to the extent technically possible, share and reuse the technical components, including hardware and software components, of the web service referred to in Article 13 of Regulation (EU) 2017/2226, the carrier gateway referred to in Article 6(2), point (k), of Regulation (EU) 2018/1240 and the carrier gateway referred to in Article 45c, of Regulation (EC) No 767/2008.

eu-LISA shall design the router, to the extent technically and operationally possible, in a way that is coherent and consistent with the obligations for air carriers set out in Regulations (EC) No 767/2008, (EU) 2017/2226 and (EU) 2018/1240.

4. The router shall automatically extract and make available the data, in accordance with Article 38 of this Regulation, to the central repository for reporting and statistics (CRRS) established by Article 39 of Regulation (EU) 2019/817.

5. eu-LISA shall design and develop the router in a way that for any transfer of API data from air carriers to the router in accordance with Article 6 and for any transmission of API data from the router to the competent border authorities in accordance with Article 14 and to the CRRS in accordance with Article 38(2) the API data are end-to-end encrypted when in transit.

Article 12

Exclusive use of the router

For the purposes of this Regulation the router shall be used only by:

(a) air carriers to transfer encrypted API data in accordance with this Regulation;

(b) the competent border authorities to receive encrypted API data in accordance with this Regulation.

This Article is without prejudice to Article 10 of Regulation (EU) 2025/13.

Article 13

Data format and transfer verifications

1. The router shall, in an automated manner and on the basis of real-time flight traffic data, verify whether the air carrier transferred the API data in accordance with Article 6(1).

2. The router shall, immediately and in an automated manner, verify whether the API data transferred to it in accordance with Article 6(1) comply with the detailed rules on the supported data formats referred to in Article 6(3).

3. Where the verification referred to in paragraph 1 of this Article determines that the data were not transferred by the air carrier or where the verification referred to in paragraph 2 of this Article determines that the data are not compliant with the detailed rules on the supported data formats, the router shall, immediately and in an automated manner, notify the air carrier concerned and the competent border authorities of the Member States to which the data were to be transmitted pursuant to Article 14(1). In such cases, the air carrier shall immediately transfer the API data in accordance with Article 6.

4. The Commission shall adopt implementing acts specifying the detailed technical and procedural rules necessary for the verifications and notifications referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 43(2).

Article 14

Transmission of API data from the router to the competent border authorities

1. Upon the data format and transfer verifications referred to in Article 13, the router shall transmit the encrypted API data transferred to it pursuant to Article 6 or Article 9(3) and (4) to the competent border authorities of the Member State or, where the flight is planned to land in one or several airports within the territories of one or more Member States to which this Regulation applies, to the competent border authorities of the Member States referred to in Article 4(3), point (c). It shall transmit those data immediately and in an automated manner, without changing their content in any way, and in accordance with the detailed rules referred to in paragraph 5 of this Article, once such rules have been adopted and are applicable.

For the purposes 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.

2. Member States shall designate competent border authorities authorised to receive the API data transmitted to them from the router in accordance with this Regulation. They shall notify, by the date of application of this Regulation referred to in Article 46, second paragraph, eu-LISA and the Commission of the name and contact details of the competent border authorities and shall, where necessary, notify eu-LISA and the Commission of any updates to that information.

The Commission shall, on the basis of those notifications and updates, compile and make publicly available a list of the notified competent border authorities, including their contact details.

3. Member States shall ensure that their competent border authorities, upon receipt of API data in accordance with paragraph 1, immediately and in an automated manner confirm receipt of such data to the router.

4. Member States shall ensure that only the duly authorised and trained staff of their competent border authorities, designated in accordance with paragraph 2, have access to the API data transmitted to them through the router. They shall lay down the necessary rules to that effect. Those rules shall include rules on the creation and regular update of a list of those staff and their profiles.

5. The Commission shall adopt implementing acts specifying the detailed technical and procedural rules necessary for the transmission of API data from the router referred to in paragraph 1 of this Article, including on requirements for data security. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 43(2).

Article 15

Deletion of API data from the router

API data transferred to the router pursuant to this Regulation shall be stored on the router only insofar as necessary to complete the transmission to the relevant competent border authorities in accordance with this Regulation and shall be deleted from the router, immediately, permanently and in an automated manner where it is confirmed, in accordance with Article 14(3), that the transmission of the API data to the relevant competent border authorities has been completed.

Article 16

Actions where it is technically impossible 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 competent border authorities 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 the air carriers and competent border authorities when it has been successfully addressed.

During the period of time between those notifications, Article 6(1) and Article 8(1) shall not apply insofar as the technical impossibility prevents the transfer of API data to the router. Air carriers shall store the API data until the technical impossibility has been successfully addressed. As soon as the technical impossibility has been successfully addressed, air carriers shall transfer the data to the router in accordance with Article 6(1).

Where the API data are received later than 96 hours after the time of departure as referred to in Article 4(3)(f), the router shall not transmit the API data to the competent border authorities, but instead delete those data.

Where it is technically impossible to use the router, and in exceptional cases related to the objectives of this Regulation that make it necessary for competent border authorities to immediately receive API data during the technical impossibility to use the router, competent border authorities may request air carriers to use any other appropriate means, ensuring the necessary level of data security, data quality and data protection, to transfer the API data directly to the competent border authorities. The competent border authorities shall process the API data received through any other appropriate means in accordance with the rules and safeguards set out in Regulation (EU) 2016/399 and applicable national law.

Following the notification from eu-LISA that the technical impossibility has been successfully addressed, and where it is confirmed in accordance with Article 14(3) that the transmission of the API data through the router to the relevant competent border authority has been completed, the competent border authority shall immediately delete the API data received by any other appropriate means.

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 23 of a Member State, the competent border authorities of that Member State shall immediately notify the air carriers, the competent authorities of the other Member States, 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 the air carriers, the competent authorities of the other Member States, eu-LISA and the Commission when it has been successfully addressed. The router shall store the API data until the technical impossibility has been successfully addressed. As soon as the technical impossibility has been successfully addressed, the router shall transmit the data in accordance with Article 14(1).

During the period of time between those notifications, Article 6(1) and Article 8(1) shall not apply insofar as the technical impossibility prevents the transfer of API data to the router. Air carriers shall store the API data until the technical impossibility has been successfully addressed. As soon as the technical impossibility has been successfully addressed, air carriers shall transfer the data to the router in accordance with Article 6(1).

Where the API data are received later than 96 hours after the time of departure as referred to in Article 4(3)(f), the router shall not transmit the API data to the competent border authorities, but instead delete those data.

Where it is technically impossible to use the router, and in exceptional cases related to the objectives of this Regulation that make it necessary for competent border authorities to immediately receive API data during the technical impossibility to use the router, competent border authorities may request air carriers to use any other appropriate means, ensuring the necessary level of data security, data quality and data protection, to transfer the API data directly to the competent border authorities. The competent border authorities shall process the API data received through any other appropriate means in accordance with the rules and safeguards set out in Regulation (EU) 2016/399 and applicable national law.

Following the notification from eu-LISA that the technical impossibility has been successfully addressed, and where it is confirmed in accordance with Article 14(3) that the transmission of the API data through the router to the relevant competent border authority has been completed, the competent border authority shall immediately delete the API data received by any other appropriate means.

3. Where it is technically impossible to use the router to transfer API data because of a failure of the systems or infrastructure referred to in Article 24 of an air carrier, that air carrier shall immediately notify the competent border authorities, 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 eu-LISA and the Commission when it has been successfully addressed.

During the period of time between those notifications, Article 6(1) and Article 8(1) shall not apply insofar as the technical impossibility prevents the transfer of API data to the router. Air carriers shall store the API data until the technical impossibility has been successfully addressed. As soon as the technical impossibility has been successfully addressed, air carriers shall transfer the data to the router in accordance with Article 6(1). However, the router shall not transmit the API data to the competent border authorities, but instead delete the data, if they are received later than 96 hours after the time of departure as referred to in Article 4(3)(f).

Where it is technically impossible to use the router, and in exceptional cases related to the objectives of this Regulation that make it necessary for competent border authorities to immediately receive API data during the technical impossibility to use the router, competent border authorities may request air carriers to use any other appropriate means, ensuring the necessary level of data security, data quality and data protection, to transfer the API data directly to the competent border authorities. The competent border authorities shall process the API data received through any other appropriate means in accordance with the rules and safeguards set out in Regulation (EU) 2016/399 and applicable national law.

Following the notification from eu-LISA that the technical impossibility has been successfully addressed, and where it is confirmed in accordance with Article 14(3) that the transmission of the API data through the router to the relevant competent border authority has been completed, the competent border authority shall immediately delete the API data received by any other appropriate means.

When the technical impossibility has been successfully addressed, the air carrier concerned shall, without delay, submit to the national API supervision authority referred to in Article 36 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.

CHAPTER 4

SPECIFIC PROVISIONS ON THE PROTECTION OF PERSONAL DATA AND SECURITY

Article 17

Keeping of logs

1. Air carriers shall create logs of all processing operations related to API data under this Regulation undertaken by using the automated means referred to in Article 5(2). Those logs shall cover the date, time and place of transfer of the API data. Those logs shall not contain any personal data, other than the information necessary to identify the relevant member of the staff of the air carrier.

2. eu-LISA shall keep logs of all processing operations relating to the transfer and transmission of API data through the router under this Regulation. Those logs shall cover:

(a) the air carrier that transferred the API data to the router;

(b) the competent border authorities to which the API data were transmitted through the router;

(c) the date and time of the transfer or transmission referred to in points (a) and (b), and the place of that transfer or transmission;

(d) any access by the staff of eu-LISA necessary for the maintenance of the router, as referred to in Article 26(3);

(e) any other information relating to those processing operations necessary to monitor the security and integrity of the API data and the lawfulness of those processing operations.

Those logs shall not include any personal data, other than the information necessary to identify the relevant member of the staff of eu-LISA, referred to in point (d) of the first subparagraph.

3. The logs referred to in paragraphs 1 and 2 of this Article 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 36 and 37.

4. Air carriers and eu-LISA shall take appropriate measures to protect the logs that they created pursuant to paragraphs 1 and 2, respectively, against unauthorised access and other security risks.

5. The national API supervision authority referred to in Article 36 and competent border authorities shall have access to the relevant logs referred to in paragraph 1 of this Article where necessary for the purposes referred to in paragraph 3 of this Article.

6. Air carriers and eu-LISA shall keep the logs that they created pursuant to paragraphs 1 and 2, respectively, for a 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 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 3, and those procedures have already begun at the moment of the expiry of the period referred to in the first subparagraph of this paragraph, eu-LISA and air carriers shall 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 18

Data protection responsibilities

1. 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 the collection of such data and the transfer thereof to the router under this Regulation.

2. Each Member State shall designate a competent authority as controller in accordance with this Article. Member States shall notify the Commission, eu-LISA and the other Member States of those authorities.

All the competent authorities designated by Member States shall be joint controllers in accordance with Article 26 of Regulation (EU) 2016/679 for the purpose of processing of personal data in the router.

3. eu-LISA shall be a processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the purposes of the processing of API data constituting personal data under this Regulation through the router, including transmission of the data from the router to the competent border authorities and storage for technical reasons of those data on the router. eu-LISA shall ensure that the router is operated in accordance with this Regulation.

4. The Commission shall adopt implementing acts establishing the respective responsibilities of the joint controllers, and the respective obligations between the joint controllers and the processor. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 43(2).

Article 19

Information for passengers

In accordance with Article 13 of Regulation (EU) 2016/679, air carriers shall 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.

That information shall 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 in accordance with Article 5.

Article 20

Security

1. eu-LISA shall ensure the security and encryption of the API data, in particular API data constituting personal data, that it processes pursuant to this Regulation. The competent border authorities and the air carriers shall ensure the security of the API data, in particular API data constituting personal data, that they process pursuant to this Regulation. eu-LISA, the competent border authorities and the air carriers shall cooperate, in accordance with their respective responsibilities and in compliance with Union law, with each other to ensure such security.

2. eu-LISA shall take the measures necessary to ensure the security of the router and the API data, in particular API data constituting personal data, transmitted through the router, including by establishing, implementing and regularly updating a security plan, a business continuity plan and a disaster recovery plan, in order to:

(a) physically protect the router, including by making contingency plans for the protection of critical components thereof;

(b) prevent any unauthorised processing of the API data, including any unauthorised access thereto and the copying, modification or deletion thereof, both during the transfer of the API data to and from the router and during any storage of the API data on the router where necessary to complete the transmission, in particular by means of appropriate encryption techniques;

(c) ensure that the persons authorised to access the router have access only to the data covered by their access authorisation;

(d) ensure that it is possible to verify and establish to which competent border authorities the API data are transmitted through the router;

(e) properly report to its Management Board any faults in the functioning of the router;

(f) monitor the effectiveness of the security measures required under this Article and under Regulation (EU) 2018/1725, and assess and update those security measures where necessary in the light of technological or operational developments.

The measures referred to in the first subparagraph of this paragraph shall not affect Article 32 of Regulation (EU) 2016/679 or Article 33 of Regulation (EU) 2018/1725.

Article 21

Self-monitoring

Air carriers and competent border authorities shall monitor their compliance with their respective obligations under this Regulation, in particular as regards their processing of API data constituting personal data. For air carriers, the monitoring shall include frequent verification of the logs referred to in Article 17(1).

Article 22

Personal data protection audits

1. The independent supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 shall carry out an audit of processing operations of API data constituting personal data performed by the competent border authorities for the purposes of this Regulation at least once every four years. Member States shall ensure that their independent supervisory authorities have sufficient resources and expertise to fulfil the tasks entrusted to them under this Regulation.

2. The European Data Protection Supervisor shall carry out an audit of processing operations of API data constituting personal data performed by eu-LISA for the purposes of this Regulation, in accordance with relevant international auditing standards at least once every year. A report of that audit shall be sent to the European Parliament, to the Council, to the Commission, to the Member States and to eu-LISA. eu-LISA shall be given an opportunity to make comments before the reports are adopted.

3. In relation to the processing operations referred to in paragraph 2 of this Article, upon request, eu-LISA shall supply information requested by the European Data Protection Supervisor, shall grant the European Data Protection Supervisor access to all the documents it requests and to the logs referred to in Article 17(2), and shall allow the European Data Protection Supervisor access to all eu-LISA's premises at any time.

CHAPTER 5

MATTERS RELATING TO THE ROUTER

Article 23

Competent border authorities' connections to the router

1. Member States shall ensure that their competent border authorities are connected to the router. They shall ensure that the competent border authorities' 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 the router and integration with it enables their competent border authorities 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 shall adopt implementing acts specifying the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1 of this Article, including on requirements for data security. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 43(2).

Article 24

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 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. To that end, air carriers shall conduct tests of the transfer of API data to the router in cooperation with eu-LISA in accordance with Article 27(3).

2. The Commission shall adopt implementing acts specifying the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1 of this Article, including on requirements for data security. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 43(2).

Article 25

eu-LISA's tasks relating to the design and development of the router

1. eu-LISA shall be responsible for the design of the physical architecture of the router, including defining its technical specifications.

2. eu-LISA shall be responsible for the development of the router, including for any technical adaptations necessary for the operation of the router.

The development of the router shall consist of the elaboration and implementation of the technical specifications, testing and overall project management and coordination of the development phase.

3. eu-LISA shall ensure that the router is designed and developed in such a manner that the router provides the functionalities specified in this Regulation, and that the router starts operations as soon as possible after the adoption by the Commission of the implementing and delegated acts provided for in Article 5(7), Article 6(3), Article 9(6), Article 23(2) and Article 24(2) of this Regulation and after the carrying out of a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679.

4. eu-LISA shall provide the competent border authorities, other relevant Member States' authorities and air carriers with a compliance test set. The compliance test set shall include a test environment, a simulator, test data sets and a test plan. The compliance test set shall allow for a comprehensive test of the router referred to in paragraph 5 and shall remain available after the completion of that test.

5. Where eu-LISA considers that the development phase has been completed, it shall, without undue delay, conduct a comprehensive test of the router, in cooperation with the competent border authorities and other relevant Member States' authorities and air carriers and inform the Commission of the outcome of that test.

Article 26

eu-LISA's tasks relating to the hosting and technical management of the router

1. eu-LISA shall host the router in its technical sites.

2. eu-LISA shall be responsible for the technical management of the router, including its maintenance and technical developments, in such a manner as to ensure that the API data are securely, effectively and swiftly transmitted through the router, in compliance with this Regulation.

The technical management of the router shall consist of carrying out all the tasks and enacting all technical solutions necessary for the proper functioning of the router in accordance with this Regulation in an uninterrupted manner, 24 hours a day, 7 days a week. It shall include the maintenance work and technical developments necessary to ensure that the router functions at a satisfactory level of technical quality, in particular as regards availability, accuracy and reliability of the transmission of API data, in accordance with the technical specifications and, as much as possible, in line with the operational needs of the competent border authorities and air carriers.

3. eu-LISA's staff shall not have access to any of the API data that are transmitted through the router. However, that prohibition shall not preclude eu-LISA's staff from having such access insofar as strictly necessary for the maintenance and technical management of the router.

4. Without prejudice to paragraph 3 of this Article and to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([28]), eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its staff required to work with API data transmitted through the router. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Article 27

eu-LISA's support tasks relating to the router

1. eu-LISA shall, upon the request of the competent border authorities, other relevant Member States' authorities or air carriers, provide training to them on the technical use of the router and on their connection and integration with the router.

2. eu-LISA shall provide support to the competent border authorities regarding the reception of API data through the router pursuant to this Regulation, in particular as regards the application of Articles 14 and 23.

3. In accordance with Article 24(1) and making use of the compliance test set referred to in Article 25(4), eu-LISA shall conduct tests of the transfer of API data to the router in cooperation with air carriers.

([28]) OJ L 56, 4.3.1968, p. 1.

CHAPTER 6

GOVERNANCE

Article 28

Programme Management Board

1. By 28 January 2025, eu-LISA's Management Board shall establish a Programme Management Board. It shall be composed of 10 members and shall consist of:

(a) seven members appointed by eu-LISA's Management Board from among its members or its alternates;

(b) the chair of the API-PNR Advisory Group referred to in Article 29;

(c) one member of the eu-LISA staff appointed by its Executive Director; and

(d) one member appointed by the Commission.

As regards point (a), the members appointed by eu-LISA's Management Board shall be elected only from its members or its alternates from those Member States to which this Regulation applies.

2. The Programme Management Board shall draft its rules of procedure to be adopted by eu-LISA's Management Board.

The chairpersonship shall be held by a Member State that is a member of the Programme Management Board.

3. The Programme Management Board shall supervise the effective fulfilment of eu-LISA's tasks relating to the design and development of the router in accordance with Article 25.

Upon request of the Programme Management Board, eu-LISA shall provide detailed and updated information on the design and development of the router, including on the resources allocated by eu-LISA.

4. The Programme Management Board shall regularly, and at least three times per quarter, submit written reports on the progress in the design and development of the router to eu-LISA's Management Board.

5. The Programme Management Board shall have no decision-making power, nor any mandate to represent eu-LISA's Management Board or its members.

6. The Programme Management Board shall cease to exist by the date of the application of this Regulation referred to in Article 46, second paragraph.

Article 29

API-PNR Advisory Group

1. As from 28 January 2025, the API-PNR Advisory Group, established pursuant to Article 27(1), point (de), of Regulation (EU) 2018/1726, shall provide eu-LISA's Management Board with the necessary expertise related to API-PNR in particular in the context of the preparation of its annual work programme and its annual activity report.

2. Whenever available, eu-LISA shall provide the API-PNR Advisory Group with versions, even intermediary ones, of the technical specifications and the compliance test sets referred to in Article 25(1), (2) and (4).

3. The API-PNR Advisory Group shall exercise the following functions:

(a) provide expertise to eu-LISA and to the Programme Management Board on the design and development of the router in accordance with Article 25;

(b) provide expertise to eu-LISA on the hosting and technical management of the router in accordance with Article 26;

(c) provide its opinion to the Programme Management Board, upon its request, on the progress of the design and development of the router, including on the progress of the technical specifications and compliance test sets referred to in paragraph 2.

4. The API-PNR Advisory Group shall have no decision-making power, nor any mandate to represent the eu-LISA's Management Board or its members.

Article 30

API-PNR Contact Group

1. By the date of the application of this Regulation referred to in Article 46, second paragraph, eu-LISA's Management Board shall establish an API-PNR Contact Group.

2. The API-PNR Contact Group shall enable communication between Member States' relevant authorities and air carriers on technical matters related to their respective tasks and obligations under this Regulation.

3. The API-PNR Contact Group shall be composed of representatives of Member States' relevant authorities and air carriers, the chairperson of the API-PNR Advisory Group and eu-LISA's experts.

4. eu-LISA's Management Board shall establish the rules of procedure of the API-PNR Contact Group, following an opinion of the API-PNR Advisory Group.

5. Where deemed necessary, eu-LISA's Management Board may also establish sub-groups of the API-PNR Contact Group to discuss specific technical matters related to the respective tasks and obligations of Member States' relevant authorities and air carriers under this Regulation.

6. The API-PNR Contact Group, including its sub-groups, shall have no decision-making power, nor any mandate to represent the eu-LISA's Management Board or its members.

Article 31

API Expert Group

1. By the date of application of this Regulation referred to in Article 46, second paragraph, the Commission shall establish an API Expert Group in accordance with the horizontal rules on the creation and operation of Commission expert groups.

2. The API Expert Group shall enable communication among Member States' relevant authorities, and between Member States' relevant authorities and air carriers, on policy matters related to their respective tasks and obligations under this Regulation, including in relation to the penalties referred to in Article 37.

3. The API Expert Group shall be chaired by the Commission and constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. It shall be composed of representatives of Member States' relevant authorities, representatives of air carriers and eu-LISA's experts. Where relevant for the performance of its tasks, the API Expert Group may invite relevant stakeholders, in particular representatives of the European Parliament, the European Data Protection Supervisor and the independent national supervisory authorities, to participate in its work.

4. The API Expert Group shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish the minutes of the meetings of the API Expert Group and other relevant documents on the Commission website.

Article 32

Costs incurred by eu-LISA, the European Data Protection Supervisor, the national supervisory authorities and Member States

1. Costs incurred by eu-LISA in relation to the establishment and operation of the router under this Regulation shall be borne by the general budget of the Union.

2. Costs incurred by the Member States in relation to the implementation of this Regulation, in particular to their connection to and the integration with the router referred to in Article 23, shall be supported by the general budget of the Union, in accordance with the eligibility rules and co-financing rates set in the applicable Union legal acts.

3. Costs incurred by the European Data Protection Supervisor in relation to the tasks entrusted to it under this Regulation shall be borne by the general budget of the Union.

4. Costs incurred by independent national supervisory authorities in relation to the tasks entrusted to them under this Regulation shall be borne by the Member States.

Article 33

Liability regarding the router

If a 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, as provided for by the applicable Union or national law, unless and insofar as it is demonstrated that eu-LISA, another Member State or another air carrier failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

Article 34

Start of operations of the router

The Commission shall determine, without undue delay, the date from which the router starts operations by means of an implementing act once eu-LISA has informed the Commission of the successful completion of the comprehensive test of the router referred to in Article 25(5). That implementing act shall be adopted in accordance with the examination procedure referred to in Article 43(2).

The Commission shall set the date referred to in the first paragraph to be no later than 30 days from the date of the adoption of that implementing act.

Article 35

Voluntary use of the router in application of Directive 2004/82/EC

1. Air carriers shall be entitled to use the router to transmit the information referred to in Article 3(1) and (2) of Directive 2004/82/EC to one or more of the responsible authorities referred to therein, in accordance with that Directive, provided that the Member State concerned has agreed with such use, from an appropriate date set by that Member State. That Member State shall agree only after having established that, in particular as regards both its own responsible authorities' connection to the router and that of the air carrier concerned, the information can be transmitted in a lawful, secure, effective and swift manner.

2. Where an air carrier starts using the router in accordance with paragraph 1 of this Article, it shall continue using the router to transmit such information to the responsible authorities of the Member State concerned until the date of application of this Regulation referred to in Article 46, second paragraph. However, that use shall be discontinued, from an appropriate date set by that Member State, where that Member State considers that there are objective reasons that require such discontinuation and has informed the air carrier accordingly.

3. The Member State concerned shall:

(a) consult eu-LISA before agreeing with the voluntary use of the router in accordance with paragraph 1;

(b) except in situations of duly justified urgency, afford the air carrier concerned an opportunity to comment on its intention to discontinue such use in accordance with paragraph 2 and, where relevant, also consult eu-LISA thereon;

(c) immediately inform eu-LISA and the Commission of any such use to which it agreed and any discontinuation of such use, providing all necessary information, including the date of the start of the use, the date of the discontinuation and the reasons for the discontinuation, as applicable.

CHAPTER 7

SUPERVISION, PENALTIES, STATISTICS AND HANDBOOK

Article 36

National API supervision authority

1. Member States shall designate one or more national API supervision 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 API supervision authorities have all the means and all the investigative and enforcement powers necessary to carry out their tasks under this Regulation, including by imposing the penalties referred to in Article 37 where appropriate. Member States shall ensure that the exercise of the powers conferred on the national API supervision authority is subject to appropriate 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 46, second paragraph, notify the Commission of the name and the contact details of the authorities that they designated under paragraph 1 of this Article. 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.

Article 37

Penalties

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

2. Member States shall, by the date of application of this Regulation referred to in Article 46, second paragraph, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. Member States shall ensure that the national API supervision authorities, when deciding whether to impose a penalty and when determining the type and level of penalty, take into account relevant circumstances, which may include:

(a) the nature, gravity and duration of the infringement;

(b) the degree of the air carrier's fault;

(c) previous infringements by the air carrier;

(d) the overall level of cooperation of the air carrier with the competent authorities;

(e) the size of the air carrier, such as the annual number of passengers carried;

(f) whether previous penalties have already been applied by other national API supervision authorities to the same air carrier for the same infringement.

4. Member States shall ensure that a recurrent failure to transfer API data in accordance with Article 6(1) is subject to proportionate financial penalties of up to 2 % of the air carrier's global turnover of the preceding financial year. Member States shall ensure that failure to comply with other obligations set out in this Regulation is subject to proportionate penalties, including financial penalties.

Article 38

Statistics

1. In order to support the implementation and monitoring of the application of this Regulation, and on the basis of the statistical information referred to in paragraph 5, eu-LISA shall publish every quarter statistics on the functioning of the router and on the compliance of air carriers with the obligations set out in this Regulation. Those statistics shall not allow for the identification of individuals.

2. For the purposes set out in paragraph 1, the router shall automatically transmit the data listed in paragraph 5 to the CRRS.

3. In order to support the implementation and monitoring of the application of this Regulation, each year eu-LISA shall compile statistical data in an annual report for the previous year. It shall publish that annual report and transmit it to the European Parliament, the Council, the Commission, the European Data Protection Supervisor, the European Border and Coast Guard Agency and the national API supervision authorities referred to in Article 36. The annual report shall not disclose confidential working methods or jeopardise ongoing investigations of the Member States' competent authorities.

4. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of this Regulation as well as the statistics pursuant to paragraph 3.

5. The CRRS shall provide eu-LISA with the following statistical information necessary for the reporting referred to in Article 45 and for generating statistics in accordance with this Article, without such statistics on API data allowing for the identification of the passengers concerned:

(a) the nationality, sex and year of birth of the passenger;

(b) the date and the initial point of embarkation, the date and airport of departure, and the date and airport of arrival;

(c) the type of travel document, the three-letter code of the issuing country and the date of expiry of the validity of the travel document;

(d) the number of passengers checked in on the same flight;

(e) the code of the air carrier operating the flight;

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

(g) whether API data were transferred immediately after flight closure;

(h) whether the personal data of the passenger are accurate, complete and up to date;

(i) the technical means used to capture the API data.

6. For the purposes of the reporting referred to in Article 45 and for generating statistics in accordance with this Article, eu-LISA shall store the data referred to in paragraph 5 of this Article in the CRRS. It shall store such data for a period of five years in accordance with paragraph 2, while ensuring that the data do not allow for the identification of the passengers concerned. The CRRS shall provide the duly authorised staff of the competent border authorities and other relevant authorities of the Member States with customisable reports and statistics on API data as referred to in paragraph 5 of this Article for the implementation and monitoring of the application of this Regulation.

7. The use of the data referred to in paragraph 5 of this Article shall not result in the profiling of individuals as referred to in Article 22 of Regulation (EU) 2016/679 or discrimination against persons on the grounds listed in Article 21 of the Charter. The data referred to in paragraph 5 of this Article shall not be used to compare or match them with personal data or to combine them with personal data.

8. The procedures put in place by eu-LISA to monitor the development and the functioning of the router referred to in Article 39(2) of Regulation (EU) 2019/817 shall include the possibility to produce regular statistics to ensure that monitoring.

Article 39

Practical handbook

The Commission shall, in close cooperation with the competent authorities and other relevant authorities of the Member States, air carriers and relevant Union bodies and agencies, prepare and make publicly available a practical handbook, containing guidelines, recommendations and best practices for the implementation of this Regulation, including on fundamental rights compliance as well as on penalties in accordance with Article 37.

The practical handbook shall take into account other relevant handbooks.

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

CHAPTER 8

RELATIONSHIP TO OTHER EXISTING INSTRUMENTS

Article 40

Repeal of Directive 2004/82/EC

Directive 2004/82/EC is repealed from the date of application of this Regulation, referred to in Article 46, second paragraph.

Article 41

Amendments to Regulation (EU) 2018/1726

Regulation (EU) 2018/1726 is amended as follows:

(1) the following article is inserted:

'*Article 13a*

Tasks related to the router

In relation to Regulations (EU) 2025/12 (*) and (EU) 2025/13 (**) of the European Parliament and of the Council, the Agency shall perform the tasks related to the router conferred on it by those Regulations.

(*) Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC (OJ L, 2025/12, 8.1.2025, ELI: http://data.europa.eu/eli/reg/2025/12/oj).

(**) Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 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 (OJ L, 2025/13, 8.1.2025, ELI: http://data.europa.eu/eli/reg/2025/13/oj).';

(2) in Article 17, paragraph 3 is replaced by the following:

'3. The seat of the Agency shall be Tallinn, Estonia.

The tasks relating to development and operational management referred to in Article 1(4) and (5), Articles 3 to 9 and Articles 11 and 13a shall be carried out at the technical site in Strasbourg, France.

A backup site capable of ensuring the operation of a large-scale IT system in the event of failure of such a system shall be installed in Sankt Johann im Pongau, Austria.';

(3) in Article 19, paragraph 1 is amended as follows:

(a) the following point is inserted:

'(eec) adopt reports on the state of play of the development of the router pursuant to Article 45(2) of Regulation (EU) 2025/12;';

(b) in point (ff), point (vi) is replaced by the following:

'(vi) the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818, and the router pursuant to Article 80(5) of Regulation (EU) 2024/982 and Article 45(5) of Regulation (EU) 2025/12;';

(c) point (hh) is replaced by the following:

'(hh) adopt formal comments on the European Data Protection Supervisor's reports on its audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240, Article 29(2) of Regulation (EU) 2019/816, Article 52 of Regulations (EU) 2019/817 and (EU) 2019/818, Article 58(1) of the Regulation (EU) 2024/982 and Article 22(3) of the Regulation (EU) 2025/12 and ensure appropriate follow-up of those audits;';

(4) in Article 27(1), the following point is inserted:

'(de) API-PNR Advisory Group.'.

Article 42

Amendment to Regulation (EU) 2019/817

In Article 39 of Regulation (EU) 2019/817, 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 EES, VIS, ETIAS and SIS, 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) 2025/12 of the European Parliament and of the Council (*).

2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240, Article 60 of Regulation (EU) 2018/1861 and Article 16 of Regulation (EU) 2018/1860, logically separated by EU information system. eu-LISA shall also collect the data and statistics from the router referred to in Article 38(1) of Regulation (EU) 2025/12. 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 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240, Article 60 of Regulation (EU) 2018/1861 and Article 45(2) of Regulation (EU) 2025/12.

(*) Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC (OJ L, 2025/12, 8.1.2025, ELI: http://data.europa.eu/eli/reg/2025/12/oj).'.

CHAPTER 9

FINAL PROVISIONS

Article 43

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), third subparagraph, of Regulation (EU) No 182/2011 shall apply.

Article 44

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 5(6) and (7), Article 6(3) and Article 9(6) shall be conferred on the Commission for a period of five years from 28 January 2025. 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.

As regards a delegated act adopted pursuant to Article 5(6), if an objection under paragraph 6 of this Article has been expressed either by the European Parliament or by the Council, the European Parliament or the Council shall not oppose the tacit extension referred to in the first subparagraph of this paragraph.

3. The delegation of power referred to in Article 5(7), Article 6(3) and Article 9(6) 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.

6. A delegated act adopted pursuant to Article 5(6) or (7), Article 6(3) or Article 9(6) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 45

Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the router in light of objectives relating to planning and costs and to monitor the functioning of the router in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. By 29 January 2026 and every year thereafter during the development phase of the router, eu-LISA shall produce a report on the state of play of the development of the router, and submit that report to the European Parliament and to the Council. The report shall contain detailed information about the costs incurred and about any risks which may impact the overall costs to be borne by the general budget of the Union in accordance with Article 32.

3. Once the router starts operations, eu-LISA shall produce a report and submit it to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved and giving reasons for any divergences.

4. By 29 January 2029 and every four years thereafter, the Commission shall produce a report containing an overall evaluation of this Regulation, including on the necessity and the added value of the collection of API data, 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 fundamental rights protected under Union law;

(d) the impact of this Regulation on the travel experience of legitimate passengers;

(e) the impact of this Regulation on the competitiveness of the aviation sector and the burden incurred by businesses;

(f) the quality of the data transmitted by the router to the competent border authorities;

(g) the performance of the router in respect of the competent border authorities.

For the purposes of point (e) of the first subparagraph, the Commission's report shall also address this Regulation's interaction with other relevant Union legislative acts, in particular Regulations (EC) No 767/2008, (EU) 2017/2226 and (EU) 2018/1240, in order to assess the overall impact of related reporting obligations on air carriers, identify provisions that could be updated and simplified, where appropriate, to mitigate the burden on air carriers, and consider actions and measures that could be taken to reduce the total cost pressure on air carriers.

5. 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.

6. The Member States and air carriers shall, upon request, provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 2, 3 and 4, such as data related to the results of the pre-checks against Union information systems and national databases performed at the external borders using API data. In particular, Member States shall provide quantitative and qualitative information on the collection of API data from an operational perspective. The information provided shall not include personal data. 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 the competent border authorities. The Commission shall ensure that any confidential information provided is appropriately protected.

Article 46

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 the date two years from the date on which the router starts operations, as determined by the Commission in accordance with Article 34.

However:

(a) Article 5(7) and (8), Article 6(3), Article 9(6), Article 13(4), Article 14(5), Article 18(4), Article 23(2), Article 24(2), Articles 25, 28 and 29, Article 32(1), and Articles 34, 43 and 44 shall apply from 28 January 2025;

(b) Article 5(6), Articles 12 and 15, Article 17(1), (3) and (4), Article 18(1), (2) and (3), and Articles 19, 20, 26, 27, 33 and 35 shall apply from the date on which the router starts operations, as determined by the Commission in accordance with Article 34.

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

Done at Brussels, 19 December 2024.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	BÓKA J.