EUROPEAN
COMMISSION

Strasbourg, 13.12.2022
COM(2022) 729 final

2022/0424 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SEC(2022) 444 final} - {SWD(2022) 421 final} - {SWD(2022) 422 final} - {SWD(2022) 423 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The last decades have witnessed an increase of people travelling by air as well as efficiency-driven innovations which result in bigger airplanes and lead to a need for more efficient passenger flows at airports. In 2019, the International Civil Aviation Organisation (ICAO) reported 4.5 billion passengers globally carried by air transport on scheduled services,[1] with over half a billion passengers that enter or leave the EU every year,[2] putting a strain on external air borders.

The processing of Advance Passenger Information (API), as provided for in the current API Directive[3] as well as this proposal, is a border management tool contributing to the effectiveness and efficiency of border checks, by facilitating and speeding up traveller clearance, as well as an instrument to counter illegal immigration. API data is a set of identity information regarding the passengers contained in their travel documents combined with flight information collected at check-in and transferred to the border authorities of the country of destination. As these authorities receive API data in advance of a flight's arrival, they can screen ahead, in accordance with the applicable legislation, travellers against risk-profiles, watchlists and databases, thus expediting border checks for persons travelling in good faith and spend more resources and time to identify travellers who need further investigation upon arrival.

The establishment of systems for the collection and transfer of API data is an international standard under the Convention on International Civil Aviation (Chicago Convention[4]) since 2017. In the EU, it is regulated by the API Directive. That Directive imposes an obligation on air carriers to transfer API data, upon request, to the border authorities of the country of destination prior to the flight's take-off. It does not impose though an obligation on Member States to request API data from air carriers, thus creating gaps and inconsistencies in the way data is collected and used, with a few Member States collecting API data systematically while others do not.[5] On average, for all Member States combined, it is estimated that API data is collected on 65% of inbound flights.[6] This creates a situation where it is easy for individuals who want to avoid checks and to bypass routes where API data is consistently collected and instead travel to their destination via flight routes where API data is less often or not at all used.

The recent API Directive evaluation demonstrated that even where Member States request API data, their national authorities do not always use API data in a consistent way. Indeed,

---

1 ICAO, The World of Air Transport in 2019, https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx.

2 Source: Eurostat (online data code: avia_paoc); these figures include the passenger transport in all current EU Member States (27 Member States).

3 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 Chicago Convention or Convention on International Civil Aviation adopted in 1944, which established the International Civil Aviation Organisation (ICAO). All Member States are parties to the Chicago Convention. ICAO Convention on International Civil Aviation.

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

6 See Impact Assessment.

API data allows border guards to perform pre-checks on the identity of passengers and the validity of the travel document used against the databases provided for in the Schengen Borders Code.[7] However, not all Member States use the API data for pre-checks against the databases set out in the Schengen Borders Code.[8] Indeed, Ireland, which is not taking part in the Schengen Borders Code, applies similar domestic legislation. That will not change as a consequence of the proposed Regulation.

The API Directive sets only limited criteria for the collection, transmission and processing of API data as regards the flight coverage for the collection of data, the data elements to be collected, or the means to capture the data – which do not take into account the evolutions in international standards and guidelines concerning API data collection.[9] This leads to very diverging practices, which hampers not only the effectiveness and efficiency of the border checks but also represents an additional burden on air carriers that need to comply with a different set of requirements depending on the routes on which they transport passengers and the Member State requesting API data. Aligning the collection and transmission of API data with these international API data standards would ensure compliance of the API requirements by the air industry. An effective use of API data requires the data to be accurate, complete and up-to-date. If identity data is not reliable and verified, which sometimes is not the case today, cross-checks in databases will not yield reliable operational results. As online check-in has become a common practice in the past 20 years, API data from a travel document is increasingly manually transcribed or "self-declared" by passengers. Incomplete, incorrect or outdated API data transferred to national authorities can lead to loopholes in the types of checks that border authorities can perform and ultimately impact travellers who can be subject to incorrect and unnecessary checks. The need to ensure that API data collected is of sufficient quality is closely linked to the means used by airlines to ensure that the relevant API data collected corresponds to information displayed on travel documents. The current API framework does not prescribe the means for collecting API data from travellers. As opposed to manually transcribed information, automated collection of the data would lead to less quality issues and a more effective and efficient use of API data, also contributing to the reduction of the time invested by competent border authorities in their interaction with carriers.

Therefore, the revision of the current legal framework on the collection and transfer of API data offers an opportunity to enhance external border management and the combating of illegal immigration. It does so by helping to ensure that every person travelling by air from a third country or a Member State not participating in the proposed Regulation to the Union (more specifically, to the States participating in the Schengen area without controls at internal borders (the 'Schengen area') as well as Ireland), meaning third-country nationals, stateless persons and EU citizens, can be pre-checked with API data prior to their arrival and that Member States apply uniform criteria as regards such collection and transfer for the purposes of the controls at the external borders and of combating illegal immigration. By facilitating

---

7 Article 8(2)(a) of the Schengen Borders Code (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) refers to the SIS, Interpol's Stolen and Lost Travel Documents (SLTD) database, and national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

8 See European Commission, Directorate-General for Migration and Home Affairs, Study on Advance Passenger Information (API): evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, Publications Office, 2020, https://data.europa.eu/doi/10.2837/882434, p. 149.

9 WCO/IATA/ICAO Guidelines on Advanced Passenger Information (API), 2014. See Annex 5 of the Impact Assessment.

passenger flows at airports and speeding up border checks, this proposal contributes to ensuring that systematic checks can be efficiently performed on every air passenger, in accordance with applicable legislation.[10]

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

This proposal addresses the need for common rules on the collection and transfer of API data for border management purposes and for combating illegal immigration, which is linked to the existence of the Schengen area and the establishment of common rules governing the movement of persons across the external borders. This proposal is consistent with obligations set out in the Schengen Borders Code on checks on persons at the external borders. The proposed Regulation comes within the wider landscape of the large-scale EU information systems that has developed substantially since the adoption of the API Directive in 2004. Additionally, the strategic guidelines adopted by the European Council in June 2014 foresee extensions of the procedures undertaken by the border guards at the external borders to increase effectiveness of checks ahead of the border control post and to limit adverse effects at the borders. These include: the Schengen Information System (SIS), the Visa Information System (VIS) and the Eurodac system.[11] In addition, three new systems are currently in development phase: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN system).[12] All these current and future systems are linked through the interoperability framework for the EU information systems[13] for security, border and migration management, adopted in 2019, and which is currently being put in place. The revisions included in this proposal take account of the interoperability framework.

In particular, the proposed router, avoids duplicating technical components by sharing components of the ETIAS carrier gateway. The ETIAS carrier gateway provides carriers with the technical means to query the ETIAS status of visa exempt third country nationals travelling to the Member States. The proposed Regulation ensures that the different data processes are differentiated and kept strictly separate and that the access rights laid down in the different EU instruments are respected. Moreover, the proposed Regulation links the work of the existing eu-LISA EES-ETIAS Advisory Group with the future work on API, building efficiency and economies of scale by avoiding duplications of working groups.

---

10 As regards the Schengen area, see European Commission, State of Schengen Report 2022, COM(2022) 301 final/2, 24.5.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0301.

11 The SIS (Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006) assists competent authorities in the EU to preserve internal security in the absence of internal border checks and the VIS allows Schengen States to exchange visa data. The Eurodac system establishes an EU asylum fingerprint database enabling Member States to compare the fingerprints of asylum applicants in order to see whether they have previously applied for asylum or entered the EU irregularly via another Member State.

12 The EES and ETIAS will strengthen security checks on travellers holding a short-term visa and those travelling visa-free to the Schengen area by enabling advance irregular migration and security vetting. The ECRIS-TCN system will address the identified gap in the exchange of information between Member States on convicted non-EU nationals.

13 Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

As explained above, the border checks that the rules of the proposed Regulation are intended to facilitate and enhance are to be conducted under the Schengen Borders Code where applicable or under national law.

In addition, generally applicable acts of EU law will apply in accordance with the conditions set out therein. Where the processing of personal data is concerned, that holds true, in particular, for the General Data Protection Regulation (GDPR)[14] and the EU Data Protection Regulation[15]. Those acts are left unaffected by the present proposal.

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

The ICAO guidelines[16] on Machine Readable Travel Documents are transposed in Regulation 2019/1157 on strengthening the security of identity cards of Union citizens and Regulation 2252/2004 on standards for security features and biometrics in passports. These Regulations are the precursors to enable an automated extraction of complete and high-quality data from travel documents.

The proposed Regulation would continue to be part of to the Schengen *acquis*. The API data will continue to be received and further processed by the competent border authorities of the Member States, solely for the purposes of border management and combating illegal immigration for which the API data was collected under the proposed Regulation.

This proposal is closely linked to the proposal for a Regulation on the collection and transfer of API data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, insofar as both proposals contain similar provisions on the list of API data elements, the collection of API data by automated means and the transfer of the data to the router.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

For the present proposed Regulation on the collection and transfer of API data for border management purposes and for combating illegal immigration, in view of the aim and the measures provided for, the appropriate legal basis is Article 77(2)(b) and (d) and Article 79(2)(c) of the Treaty on the Functioning of the European Union (TFEU).

Under point (b) of paragraph 2 of Article 77 TFEU, the Union has the power to adopt measures relating to the checks to which persons crossing external borders are subject, and under point (d) the Union has the power to adopt any measure necessary for the gradual

[14] 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.

[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).

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

establishment of an integrated management for external borders. Under point (c) of paragraph 2 of Article 79 TFEU, the Union has the power to adopt measures relating to illegal immigration.

In this manner, consistency is ensured with the current API Directive, which is based on the same provisions.

- **Subsidiarity**

The TFEU explicitly empowering the Union to develop a common policy on the checks to which persons crossing external borders are subject, this is a clear objective to be pursued at EU level. At the same time, this is an area of shared competence between the EU and the Member States.

The need for common rules on the collection and transfer of API data for border management and combating illegal immigration is linked, in particular and without prejudice to Ireland's specific position, to the creation of the Schengen area and the establishment of common rules governing the movement of persons across the external borders, in particular with the Schengen Borders Code.[17] In this context, the decisions of one Member State affect other Member States, therefore it is necessary to have common and clear rules and operational practices in this area. Efficient and effective external border controls require a coherent approach across the entire Schengen area, including on the possibility of pre-checks of travellers with API data.

The need for EU action on API data at this point in time also stems from recent legislative developments on Schengen external border management, notably:

– The 2019 Interoperability Regulation[18] will enable systematic checks of persons crossing the external borders against all available and relevant information in EU centralised information systems for security, border and migration management. Establishing a centralised transmission mechanism for API data at EU level is a logical continuation of this concept. Following the concepts included in the Interoperability Regulations, the centralised transmission of API data could in the future lead to using this data to query various databases (SIS, Europol data) via the European Search Portal.

– At the external borders, the use of API data would effectively complement the imminent implementation of the European Travel Information and Authorisation System (ETIAS) and of the Entry Exit System (EES). The use of API data would remain necessary for external border management as it informs border guards in advance whether a traveller has effectively boarded a plane and is about to enter the Schengen area, thus facilitating the border check that will take place once that traveller arrives at the external borders.

- **Proportionality**

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

[17] 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).

[18] 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.

action enabling Member States to tackle these problems effectively without going beyond what is necessary to tackle those problems.

With this proposal, the legal framework for the collection and transfer of API data for the purposes of external border management and combating illegal immigration will be reinforced. It will strengthen the API data as an instrument enhancing the pre-checks of travellers at external borders, thus contributing not only to the effectiveness and efficiency of the checks themselves, but also to the aim of tackling illegal immigration, specifically in connection to cross-border air travel and the responsibilities of the air carriers in this regard. In alignment with international standards and recommended practices, this proposal will require air carriers to collect and transfer API data for all flights into the Union, as defined in the proposal. The obligations set out in this proposal are limited to what is necessary to achieve this objective. More specifically, this proposal establishes clear rules, among others, on what constitutes API data, on which flights air carriers should collect API data and the transfer thereof. By way of a Regulation, this proposal will establish a consistent approach to the use of API data for external border management and combating illegal immigration. Such standardisation of API requirements across Member States will contribute to increased legal certainty and foreseeability, and therefore also increased compliance by air carriers.

Proportionality is further ensured through several elements of the proposed Regulation, such as the limitation only to incoming flights, the targeting of the requirement to use automated means to only certain API data and safeguards as regards the manner and purpose of the processing of API data.

The proposed Regulation envisages the creation of a router that would serve as a single connecting point between Member States and air carriers, in line with international recommendations and it establishes an EU approach for the collection and transmission of API data. The transmission of API data through the router will reduce costs on the air industry and would ensure that border guards have access to fast and seamless access to API data they need to perform in the context of advanced border checks. This approach will drastically reduce the number of connections to establish and maintain from a Member States' perspective. Conversely, this will reduce the complexity for air carriers to maintain connections with competent border authorities and introduce economies of scale. An EU Agency, namely eu-LISA, will be responsible for the design, development, hosting and technical management of the router. The transfer of the API data through the router will support the monitoring of flights and thus reduce the probability that a carrier did not comply with the obligation to communicate API data as prescribed in this proposal.

- **Choice of the instrument**

A Regulation is proposed. As assessed in the impact assessment accompanying this proposal and in view of the need for the proposed measures to be directly applicable and uniformly applied across Member States, a Regulation is the appropriate choice of legal instrument.

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

• Ex-post evaluations of existing legislation

The evaluation of the API Directive[19] found that the rationale for collecting API data and transferring it to the competent border authorities is still valid 15 years after the entry into force of the Directive. The current objectives of the Directive, notably improving border control management, which can in turn also help combating irregular migration, remain highly pertinent to the needs of the relevant stakeholders and the wider societies. In addition, collecting and transferring API data was also found relevant to facilitate legitimate travel.

The evaluation found that the lack of harmonisation in the implementation of the Directive is an obstacle to its effectiveness and coherence. As a result of the minimum requirements imposed by the Directive, the implementation of API systems, and also the actual usage of API data, show a fragmented picture. In addition, the option left to Member States in connection to the use of API data for law enforcement purposes,[20] without providing a clear definition of this purpose nor laying down a framework, led to a disjointed implementation at national level. The evaluation also found discrepancies with other EU instruments causing operational challenges in practice and uncertainty for affected parties, in particular data subjects. The personal data protection requirements contained in the API Directive are not fully in line with the most recent developments in the field. Furthermore, the API Directive is not fully coherent with the international regulatory framework on passenger information, especially as concerns data fields and transmission standards.

The evaluation highlighted a number of shortcomings related to the API Directive, i.e. the lack of (i) standardisation and harmonisation, (ii) certain data protection safeguards and (iii) clear alignment with the latest policy and legal developments at EU level. These elements affect the impact of the Directive, create burden on the stakeholders and generate a certain level of legal uncertainty, both for the air carriers collecting and transferring the API data, for the competent border authorities receiving and further processing them, and ultimately for the passengers.

The findings of the evaluation supported the preparation of the impact assessment and of this proposal.

• Stakeholder consultations

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

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

[20] See Article 6, last subparagraph, of the API Directive.

consultation carried out end of 2019 within the framework of the evaluation of the API Directive.[21]

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

An inception impact assessment was published for feedback from 5 June 2020 to 14 August 2020, with a total of seven contributions received providing feedback on the extension of the scope of the future API Directive, data quality, sanctions, relation of API and PNR data, and protection of personal data.[22]

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

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

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

- **Impact assessment**

In line with the Better Regulation Guidelines, the Commission conducted an Impact Assessment, as presented in the accompanying Staff Working document.[23] The Regulatory Scrutiny Board reviewed the draft impact assessment at its meeting of 28 September 2022 and delivered its positive opinion on 30 September 2022.

In view of the problems identified in respect of the collection and transfer of API data, the Impact Assessment evaluated policy options on the scope of collection of API data for the abovementioned purposes, together with options on the means to improving the quality of API data. As regards the collection of API data for external border management and combating illegal immigration, the impact assessment considered the collection of API data on all extra-Schengen inbound flights on the one hand, and the collection of API data on all extra-Schengen inbound and outbound flights on the other hand. In addition, the Impact Assessment also considered options to improve the quality of API data – either to collect API data using automated and manual means, or to collect API data using automated means only.

As the full API data set is generated once the passengers are on board of a plane, the border guards would only receive the API data after the physical exit checks of the travellers and examination of their passports, and hence too late to support the work of the border guards,

---

21 Evaluation of the API Directive, SWD(2020)174.

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

23 SWD(2022) 422 final (13.12.2022).

hence the option for the collection of API data on all relevant inbound and outbound flights was not selected as part of the preferred option.

Based on the findings of the Impact Assessment report, the preferred option for an API instrument for said purposes includes the collection of API data on all relevant inbound flights, with the collection by air carriers of certain API data by automated means only. A combination of these options would improve Member States' capacity to use API data to effectively and efficiently pre-check air travellers ahead of their arrival at external borders. A standardisation of the requirements for the collection and transfer of API data would increase compliance of airline industry as it would be faced with the same requirements in all Member States. More reliable and verified API data, including the API data collected by automated means would allow for the identification of high-risk travellers and ensure a speedier facilitation of external border checks and clearance of passengers upon arrival. The proposal is consistent with the climate-neutrality objective set out in the European Climate Law[24] and the Union 2030 and 2040 targets.

The Impact Assessment also considered – and discarded – options such as the collection of API data from other means of transport, such as maritime, rail and bus transport operators. The Impact Assessment set out that there are already EU and international rules requiring maritime transport operators to transfer passenger information in advance to Member States' border authorities on incoming and outgoing routes. An additional EU obligation on maritime transport operators to transfer API data would therefore be redundant. Compared to the air transport sector, the collection of passenger data is more challenging for land transport operators such as rail or bus (absence of check-in processes, no systematic issuance of nominative tickets) and would require heavy investments in the physical infrastructure of operators, with substantial consequences on their economic model and on passengers. The decision not to cover these aspects in the present proposed Regulation is without prejudice to practices of some Member States requesting passenger data on rail connections based on national law, provided they comply with EU law.

- **Fundamental rights and protection of personal data**

This initiative provides for the processing of personal data of travellers and therefore limits the exercise of the fundamental right to the protection of personal data as guaranteed by Article 8 of the Charter of Fundamental Rights of the EU ('Charter') and Article 16 of the TFEU. As underlined by the Court of Justice of the EU (CJEU),[25] the right to the protection of personal data is not an absolute right, but any limitation must be considered in relation to its function in society and comply with the criteria set out in Article 52(1) of the Charter.[26] Personal data protection is also closely linked to respect for the right to privacy, as part of the right to private and family life protected by Article 7 of the Charter.

---

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

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

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

The obligation on air carriers to collect API data on all travellers crossing the external borders and subsequently transfer that API data, via the router, to the competent border authorities corresponds to the objective of helping to ensure that pre-checks at external borders are carried out effectively and efficiently on all travellers entering Member States, thus also contributing to the objective of combating illegal immigration. While no decisions will be taken by competent border authorities solely based on API data, this proposal will enable border authorities to organise their activities in advance and facilitate the entry of bona fide passengers and the detection of other passengers. The interference with the aforementioned fundamental rights is limited to what is strictly necessary to achieve the objectives mentioned, in particular by limiting the collection of identity data to information contained in the travellers' travel document and by limiting the extent of the processing to the minimum necessary, including as regards the time period during which personal data is kept.

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

This proposal also includes additional and specific safeguards to ensure compliance with the Charter, including as regards the security of processing of personal data, deletion and purpose limitation and the travellers' right of information.

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

4. BUDGETARY IMPLICATIONS

This legislative initiative on the collection and transfer of API data for facilitating external border controls would have an impact on the budget and staff needs of eu-LISA and Member States' competent border authorities.

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

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

Management and Visa Instrument fund[27]. Any such entitlement will ultimately have to be determined in accordance with the rules regulating those funds as well as the rules on costs contained in the proposed Regulation.

In view of the close connection between this proposed Regulation and the proposed Regulation for the collection and transfer of API data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, particularly as regards the transfer of API data to the router, the legislative financial statement, in annex of this proposed Regulation, is identical to both proposals.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

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

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

• Variable geometry

This proposal builds upon and develops the Schengen *acquis* regarding external borders in that it concerns the crossing of external borders. Therefore, the following consequences in relation to Protocol (No 19) on the Schengen acquis integrated into the framework of the European Union annexed to the TEU and to the TFEU and Protocol (No 22) on the Position of Denmark annexed to the TEU and to the TFEU should be considered.

The proposal is covered by the measures of the Schengen *acquis* in which Ireland takes part in accordance with Article 6(2) of 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*[28]. Specifically, the participation of Ireland in this proposal relates to the responsibilities of the Union for taking measures developing the provisions of the Schengen *acquis* against illegal immigration in which Ireland participates. Ireland participates, in particular, in view of the inclusion in Article 1(1) of that Council Decision of a reference to Article 26 of the Convention implementing the Schengen Convention regarding air carriers' responsibilities in respect of aliens who are refused entry and alien's possession of the required travel documents. Ireland participates in the entire proposed Regulation.

---

[27] Regulation (EU) 2021/1148 of the European Parliament and of the Council of 7 July 2021 establishing, as part of the Integrated Border Management Fund, the Instrument for Financial Support for Border Management and Visa Policy.

[28] OJ L 64, 7.3.2002, p. 20.

In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union (TEU) and to the TFEU, Denmark will not take part in the adoption of this proposal and is not bound by it or subject to its application once adopted. Given that the proposed Regulation will build upon the Schengen *acquis*, Denmark is, in accordance with Article 4 of that Protocol, to decide within a period of six months after the Council has decided on this proposal whether it will implement it in its national law.

As regards Cyprus, Bulgaria and Romania and Croatia, the proposed Regulation will constitute an act building upon, or otherwise relating to, the Schengen *acquis* within, the meaning of, respectively, Article 3(1) of the 2003 Act of Accession, Article 4(1) of the 2005 Act of Accession and Article 4(1) of the 2011 Act of Accession.

With regard to Iceland, Norway, Switzerland and Liechtenstein the proposed Regulation will constitute a development of provisions of the Schengen *acquis* within the meaning of their respective Association Agreements.

- **Detailed explanation of the specific provisions of the proposal**

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

Chapter 2 sets out the provisions for the collection and transfer of API data, namely a clear set of rules for the collection of API data by air carriers, rules regarding the transfer of API data to the router, the processing of API data by competent border authorities, and the storage and deletion of API data by air carriers and those authorities.

Chapter 3 contains provisions for the transmission of API data through the router. More specifically, it includes provisions describing the main features of the router, rules on the use of the router, the procedure for the transmission of API data from the router to the competent border authorities, deletion of API data from the router, the keeping of logs, and the procedures in case of a partial or full technical impossibility to use the router.

Chapter 4 on contains a set of specific provisions on the protection of personal data. More specifically, it specifies who the data controllers and data processor are for the processing of API data constituting personal data pursuant to this Regulation. It also sets out measures required from eu-LISA to ensure the security of data processing, in line with the provisions of Regulation (EU) 2018/1725. It sets out measures required from air carriers and competent border authorities to ensure their self-monitoring of compliance with the relevant provisions set out in this Regulation and rules on audits.

Chapter 5 regulates certain specific issues relating to the router. It contains requirements on the connections to the router of competent border authorities and air carriers. It also sets out the tasks of eu-LISA relating to the design and development of, the hosting and technical management of, and other support tasks relating to, the router. The chapter additionally contains provisions concerning the costs incurred by eu-LISA and Member States under this Regulation, in particular as regards Member States' connections to and integration with the router. It also sets out provisions regarding liability for damage cause to the router, the start of operations of the router and the possibility of voluntary use of the router by air carriers subject to certain conditions.

Chapter 6 contains provisions on supervision, possible penalties applicable to air carriers for non-compliance of their obligations set out in this Regulation, rules relating to statistical reporting by eu-LISA, and on the preparation of a practical handbook by the Commission.

Chapter 7 regulates the effects on other acts of EU law. More specifically, it contains the provisions concerning the repeal of Directive 2004/82/EC and the necessary amendments to

other existing instruments, namely Regulation (EU) 2018/1726[29] and Regulation (EU) 2019/817.[30]

Chapter 8 contains the final provisions of this Regulation, which concern the adoption of delegated and implementing acts, the monitoring and evaluation of this Regulation, and its entry into force and application.

[29] 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).

[30] 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).

2022/0424 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

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[31],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The carrying-out of checks of persons at the external borders significantly contributes to guaranteeing the long-term security of the Union, Member States and its citizens and, as such, remains an important safeguard, especially in the area without internal border control ('the Schengen area'). Efficient and effective external border controls, carried out in accordance with, in particular, Regulation (EU) 2016/399 of the European Parliament and of the Council[32] where applicable, help combating illegal immigration and prevent threats to the Member States' internal security, public policy, public health and international relations.

(2) The use of traveller data and flight information transferred ahead of the arrival of travellers, known as advance passenger information ('API') data, contributes to speeding up the process of carrying out the required 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 not participating in this Regulation, on the one hand, and a Member State participating in this Regulation, on the other hand. Such use strengthens checks at those external borders by providing sufficient time to enable detailed and comprehensive checks to be carried out on all travellers, without having a disproportionate negative effect on persons travelling in good faith. Therefore, in the interest of the effectiveness and efficiency of 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 travellers.

---

31 [OJ C , , p. .]

32 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).

(3) The existing legal framework on API data, which consists of Council Directive 2004/82/EC[33] and national law transposing that Directive, has proven important in improving border controls, notably 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, divergences remain at national level. In particular, API data is 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 needs to be transferred to competent border authorities. Those divergences lead not only to unnecessary costs and complications for the air carriers, but they are also prejudicial to ensuring effective and efficient pre-checks of persons arriving at external borders.

(4) The existing legal framework should therefore 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.

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

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

(7) In order to achieve its objectives, this Regulation should apply to all carriers conducting flights into the Union, as defined in this Regulation, covering both scheduled and non-scheduled flights, irrespective of the place of establishment of the air carriers conducting those flights.

(8) In the interest of effectiveness and legal certainty, the items of information that jointly 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 traveller and information on the flight of that traveller. Such flight information should cover information on the border crossing point of entry into the territory of the Member State concerned in all cases covered by this Regulation, but that information should be collected only where applicable under Regulation (EU) [API law enforcement], that is, not when the API data relate to intra-EU flights.

---

[33] 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).

(9) 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. However, considering that suitable technological solutions exist that allow collecting certain API data automatically while guaranteeing that the API data concerned is accurate, complete and up-to-date, and having regard the advantages of the use of such technology in terms of effectiveness and efficiency, air carriers should be required to collect that API data using automated means, by reading information from the machine-readable data of the travel document.

(10) Automated means enable travellers to provide certain API data themselves during an online check-in process. Such means could, for example, include a secure app on a travellers' smartphone, computer or webcam with the capability to read the machine-readable data of the travel document. Where the travellers did not check-in online, air carriers should in practice provide them with the possibility to provide the machine-readable API data concerned during check-in at the airport with the assistance of a self-service kiosk or of airline staff at the counter.

(11) The Commission should be empowered to adopt technical requirements and procedural rules that air carriers are to comply with in connection to the use of automated means for the collection of machine-readable API data under this Regulation, so as to increase clarity and legal certainty and contribute to ensuring data quality and the responsible use of the automated means.

(12) 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, it should be clarified that air carriers that decide to use automated means to collect the information that they are required to transmit under Directive 2004//82/EC have the possibility, but not the obligation, to apply those requirements, once adopted, in connection to such use of automated means, insofar as that Directive permits. 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 the air carriers and the Member States under that Directive.

(13) In view of 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 data of travellers that are effectively set to cross the external borders, that is, of travellers that are effectively on board of the aircraft. Therefore, the air carriers should transfer API data directly after flight closure. Moreover, API data helps the competent border authorities to distinguish legitimate travellers from travellers who may be of interest and therefore may 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 unexpected number of travellers of interest whose physical checks at the borders could adversely affect the border checks and waiting times at the borders of other legitimate travellers. To provide the competent border authorities with an opportunity to prepare adequate and proportionate measures at the border, such as temporarily reinforcing or reaffecting 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 transmitted prior to boarding, at the moment of check-in of each traveller.

(14) 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, the Commission should be empowered to lay down specifications on the common protocols and supported data formats to be used for those transfers.

(15) 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 other purpose than enhancing and facilitating the effectiveness and efficiency of border checks at external borders and combating illegal immigration.

(16) To ensure that competent border authorities have sufficient time to carry out pre-checks effectively on all travellers, including travellers 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 the air carriers is complete, accurate and up-to-date, and where necessary to request additional clarifications, corrections or completions from the air carriers, the competent border authorities should store the API data that they received under this Regulation for a fixed time period that remains limited to what is strictly necessary for those purposes. Similarly, to be able to respond to such requests, air carriers should store the API data that they transferred under this Regulation for the same fixed and strictly necessary time period.

(17) In order to avoid that 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 the related inefficiencies and security risks, provision should be made for a single router, created and operated at Union level, 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 respect of the rules of this Regulation and Regulation (EU) [API law enforcement], rely on technical components from other relevant systems created under Union law.

(18) 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. To ensure the proper functioning of this Regulation and in the interest of transparency, that information should be made public.

(19) The router should serve only to facilitate the transmission of API data from the air carriers to the competent border authorities in accordance with this Regulation and to PIUs in accordance with Regulation (EU) [API law enforcement], 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, any storage of the API data on the router should remain limited to what is 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 or, where relevant under Regulation (EU) [API law enforcement], the API data is not to be transmitted at all.

(20) With a view to ensuring the proper functioning of the transmission of API data from router, the Commission should be empowered to lay down detailed technical and

procedural rules on that transmission. Those rules should be such as to ensure that the transmission is secure, effective and swift and impacts passengers' travel and air carriers no more than necessary.

(21) 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 to gain experience in using it, air carriers should be provided with the possibility, but not the obligation, to use the router to transmit the information that they are required to transmit 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 responsible authority that is to receive the information should be required, upon request of the air carrier and after that authority 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 for the transmission of the information to the responsible authority concerned, such as it having become apparent that the information is not transmitted in a lawful, secure, effective and swift manner. In the interest of the proper application of this possibility 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. 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 the air carriers and the Member States under that Directive.

(22) The router to be created and operated under this Regulation should reduce and simplify the technical connections needed to transfer API data, limiting them to a single connection per air carrier and per competent border authority. Therefore, this Regulation provides 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, so as to ensure that the system for transferring API data established by this Regulation can function properly. To give effect to those obligations and to ensure the proper functioning of the system set up by this Regulation, they should be supplemented by detailed rules.

(23) In view of the Union interests at stake, the costs incurred by eu-LISA for the performance of its tasks under this Regulation and Regulation (EU) [API law enforcement] in respect of the router should be borne by the Union budget. The same should go for appropriate costs incurred by the Member States in relation to their connections to, and integration with, the router, as required under this Regulation and in accordance with the applicable legislation, subject to certain exceptions. The costs covered by those exceptions should be borne by each Member State concerned itself.

(24) It cannot be excluded that, due to exceptional circumstances and despite all reasonable measures having been taken in accordance with this Regulation, the router or the systems or infrastructure connecting the competent border authorities and the air carriers thereto fail to function properly, thus leading to a technical impossibility to use the router to transmit API data. Given the unavailability of the router and that it will generally not be reasonably possible for air carriers to transfer the API data affected by the failure in a lawful, secure, effective and swift manner through alternative means, the obligation for air carriers to transfer that API data to the router

should cease to apply for as long as the technical impossibility persist. In order to minimise the duration and negative consequences thereof, the parties concerned should in such a case immediately inform each other and immediately take all necessary measures to address the technical impossibility. Considering that API data relating to flights that already arrived is not useful for border checks, there is in such a case no justification for requring the air carriers to collect and store the API data. This arrangement should be without prejudice to the obligations under this Regulation of all parties concerned to ensure that the router and their respective systems and infrastructure function properly, as well as the fact that air carriers are subject to penalties when they fail to meet those obligations, including when they seek to rely on this arrangement where such reliance is not justified. In order to deter such abuse and to facilitate supervision and, where necessary, the imposition of penalties, air carriers that rely on this arrangement on account of the failure of their own system and infrastructure should report thereon to the competent supervisory authority.

(25) 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 understood as complementing the generally applicable acts of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[34] and Regulation (EU) 2018/1725 of the European Parliament and the Council.[35] Those acts, which also apply to the processing of personal data under this Regulation in accordance with the provisions thereof, should not be affected by this Regulation.

(26) In particular, 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, the competent border authorities receiving the API data should be controllers for the transmission of API data constituting personal data via router and the storage of that data on the router insofar as such storage is needed for technical purposes, and for any of their processing subsequently using that data to enhance and facilitate border checks at external borders. The air carriers, in turn, should be separate controllers regarding the processing of API data constituting personal data that they are obliged to undertake under this Regulation. On this basis, both the air carriers and the competent border authorities should be separate data controllers with regard to their own respective processing of API data under this Regulation.

(27) 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

---

[34] 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).

[35] 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).

authorities charged with the supervision of those rules. The rules of this Regulation on such supervision, including as regards the imposition of penalties where necessary, should leave the tasks and powers of the supervisory authorities established in accordance with Regulation (EU) 2016/679 unaffected, including in relation to the processing of personal data under this Regulation.

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

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

(30) As the router should be designed, developed, hosted and technically managed by the eu-LISA, established by Regulation (EU) 2018/1726 of the European Parliament and of the Council[36], it is necessary to amend that Regulation by adding that task to the tasks of eu-LISA. In order to store reports and statistics of the router on the Common Repository for Reporting and Statistics it is necessary to amend Regulation (EU) 2019/817 of the European Parliament and of the Council[37].

(31) In order to adopt measures relating to the technical requirements and operational rules for the automated means for the collection of machine-readable API data, to the common protocols and formats to be used for the transfer of API data by air carriers, to the technical and procedural rules for the transmission of API data from the router to the competent border authorities and to the PIUs and to the PIU's and air carriers' connections to and integration with the router, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of Articles 5, 6, 11, 20 and 21 respectively. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[38]. 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.

(32) In order to ensure uniform conditions for the implementation of this Regulation, namely as regards the start of operations of the router, implementing powers should be

---

[36] 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).

[37] 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).

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

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[39].

(33) All interested parties, and in particular the air carriers and the competent border authorities, should be afforded sufficient time to make the necessary preparations to be able to meet their respective obligations under this Regulation, taking into account that some of those preparations, such as those regarding the obligations on the connection to and integration with the router, can only be finalised when the design and development phases of the router have been completed and the router starts operations. Therefore, this Regulation should apply only from an appropriate date after the date at which the router starts operations, as specified by the Commission in accordance with this Regulation.

(34) However, the design and development phases of the router 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 implementing and delegated acts provided for by this Regulation. 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 articles 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 article on such use, as well as certain other articles 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.

(35) This Regulation should not affect the possibility for Member States to provide, under their national law, for a system of collecting API data from transportation providers other than those specified in this Regulation, provided that such national law complies with Union law.

(36) 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 the European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(37) 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.

(38) 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,

[39] 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).

annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and Article 6(2) of Council Decision 2002/192/EC.[40]

(39) The participation of Ireland in this Regulation in accordance with Article 6(2) of Decision 2002/192/EC relates to the responsibilities of the Union for taking measures developing the provisions of the Schengen *acquis* against illegal immigration in which Ireland participates.

(40) 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 association of those two States with the implementation, application and development of the Schengen *acquis*[41], which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[42].

(41) 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*[43], 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[44].

(42) 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 with the implementation, application and development of the Schengen *acquis*[45] which fall within the area referred to in Article 1, point A, of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[46].

(43) As regards Cyprus, Bulgaria and Romania and Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively,

---

40 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).

41 OJ L 176, 10.7.1999, p. 36.

42 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).

43 OJ L 53, 27.2.2008, p. 52.

44 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).

45 OJ L 160, 18.6.2011, p. 21.

46 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).

the meaning of Article 3(1) of the 2003 Act of Accession, Article 4(1) of the 2005 Act of Accession and Article 4(1) of the 2011 Act of Accession.

(44) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on [XX],[47]

HAVE ADOPTED THIS REGULATION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

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

(a) the collection by air carriers of advance passenger information ('API data') on flights into the Union;

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

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

Article 2

Scope

This Regulation applies to air carriers conducting scheduled or non-scheduled flights into the Union.

Article 3

Definitions

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

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

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

(c) 'flights into the Union' means flights flying from the territory either of a third country or of a Member State not participating in this Regulation, and planned to land on the territory of a Member State participating in this Regulation;

(d) 'border crossing point' means the crossing point as defined in Article 2, point 8, of Regulation (EU) 2016/399;

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

[47] [OJ C …]

(f) ‘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;

(g) ‘competent border authority’ means the authority charged by a Member State to carry out border checks and designated and notified by that Member State in accordance with Article 11(2);

(h) ‘passenger’ means any person, excluding 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 passengers list;

(i) ‘crew’ means any person on board of an aircraft during the flight, other than a passenger, who works on and operates the aircraft, including flight crew and cabin crew;

(j) ‘traveller’ means a passenger or crew member;

(k) ‘Advance Passenger Information data’ or ‘API data’ means the traveller data and the flight information referred to in Article 4(2) and (3) respectively;

(l) ‘Passenger Information Unit’ or ‘PIU’ means the competent authority referred to in Article 3, point i, of Regulation (EU) [API law enforcement];

(m) ‘the router’ means the router referred to in Article 9;

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

CHAPTER 2

COLLECTION AND TRANSFER OF API DATA

Article 4

API data to be collected by air carriers

1. Air carriers shall collect API data of travellers, consisting of the traveller data and the flight information specified in paragraphs 2 and 3 of this Article, respectively, on the flights referred to in Article 2, for the purpose of transferring that API data to the router in accordance with Article 6.

2. The API data shall consist of the following traveller data relating to each traveller 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) whether the traveller is a passenger or a crew member (traveller’s status);

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

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

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

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

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

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

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

(d) the initial point of embarkation;

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

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

Article 5

Means of collecting API data

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

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

However, where such use of automated means is not possible due to the travel document not containing machine-readable data, air carriers shall collect that data manually, in such a manner as to ensure compliance with paragraph 1.

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

4. The Commission is empowered to adopt delegated acts in accordance with Article 37 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 paragraph 2 and 3 of this Article.

5. Air carriers that use automated means to collect the information referred to in Article 3(1) of Directive 2004/82/EC shall be entitled to do so applying the technical requirements relating to such use referred to in paragraph 4, in accordance with that Directive.

Article 6

Obligations on air carriers regarding transfers of API data

1. Air carriers shall transfer the API data to the router by electronic means. They shall do so in accordance with the detailed rules referred to in paragraph 3, where such rules have been adopted and are applicable.

2. Air carriers shall transfer the API data both at the moment of check-in and immediately after flight closure, that is, 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 37 to supplement this Regulation by laying down the necessary detailed rules on the common protocols and supported data formats to be used for the transfers of API data to the router referred to in paragraph 1.

4. Where an air carrier becomes aware, after having transferred data to the router, that the API data is inaccurate, incomplete, no longer up-to-date or was processed unlawfully, or that the data does not constitute API data, it 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 API data transmitted through the router.

Article 7

Processing of API data received

The competent border authorities shall process API data, transferred to them in accordance with this Regulation, solely for the purposes referred to in Article 1.

Article 8

Storage and deletion of API data

1. Air carriers shall store, for a time period of 48 hours from the moment of departure of the flight, the API data relating to that passenger that they collected pursuant to Article 4. They shall immediately and permanently delete that API data after the expiry of that time period.

2. The competent border authorities shall store, for a time period of 48 hours from the moment of departure of the flight, the API data relating to that passenger that they received through the router pursuant to Article 11. They shall immediately and permanently delete that API data after the expiry of that time period.

3. Where an air carrier or competent border authority becomes aware that the data that it has collected, transferred or received under to this Regulation is inaccurate, incomplete, no longer up-to-date or was processed unlawfully, or that the data does not constitute API data, it shall immediately either correct, complete or update, or permanently delete, that API 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.

CHAPTER 3

PROVISIONS RELATING TO THE ROUTER

Article 9

The router

1. eu-LISA shall design, develop, host and technically manage, in accordance with Articles 22 and 23, a router for the purpose of facilitating the transfer of API data by the air carriers to the competent border authorities and to the PIUs in accordance with this Regulation and Regulation (EU) [API law enforcement], respectively.

2. The router shall be composed of:

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

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

3. Without prejudice to Article 10 of this Regulation, the router shall, to the extent technically possible, share and re-use the technical components, including hardware and software components, of the web service referred to in Article 13 of Regulation (EU) 2017/2226 of the European Parliament and of the Council[48], the carrier gateway referred to in Article 6(2), point (k), of Regulation (EU) 2018/1240, and the carrier gateway referred to in Article 2a, point (h), of Regulation (EC) 767/2008 of the European Parliament and of the Council[49].

Article 10

Exclusive use of the router

The router shall only be used by air carriers to transfer API data and by competent border authorities and PIUs to receive API data, in accordance with this Regulation and Regulation (EU) [API law enforcement], respectively.

Article 11

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

1. The router shall, immediately and in an automated manner, transmit the API data, transferred to it pursuant to Article 6, to the competent border authorities of the Member State referred to in Article 4(3), point (c). It shall do so in accordance with the detailed rules referred to in paragraph 4 of this Article, where such rules have been adopted and are applicable.

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

---

48 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).

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

2. The Member State shall designate the competent border authorities authorised to receive the API data transferred 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 39, second subparagraph, eu-LISA and the Commission of the name and contact details of the competent border authorities and shall, where necessary, update the notified 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. The Member States shall ensure that only the duly authorised staff of the competent border authorities 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.

4. The Commission is empowered to adopt delegated acts in accordance with Article 37 to supplement this Regulation by laying down the necessary detailed technical and procedural rules for the transmissions of API data from the router referred to in paragraph 1.

Article 12

Deletion of API data from the router

API data, transferred to the router pursuant to this Regulation and Regulation (EU) [API law enforcement], shall be stored on the router only insofar as necessary to complete the transmission to the relevant competent borders authorities or PIUs, as applicable, in accordance with those Regulations and shall be deleted from the router, immediately, permanently and in an automated manner, in both of the following situations:

(a) where the transmission of the API data to the relevant competent border authorities or PIUs, as applicable, has been completed;

(b) in respect of Regulation (EU) [API law enforcement], where the API data relates to other intra-EU flights than those included the lists referred to in Article 5(2) of that Regulation.

Article 13

Keeping of logs

1. eu-LISA shall keep logs of all processing operations relating to the transfer of API data through the router under this Regulation and Regulation (EU) [API law enforcement]. Those logs shall cover the following:

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

(b) the competent border authorities and PIUs to which the API data was transmitted through the router;

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

(d) any access by staff of eu-LISA necessary for the maintenance of the router, as refererred to in Article 23(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.

2. Air carriers shall create logs of all processing operations 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.

3. The logs referred to in paragraphs 1 and 2 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 and Regulation (EU) [API Law Enforcement], including proceedings for penalties for infringements of those requirements in accordance with Articles 29 and 30 of this Regulation.

4. eu-LISA and the air carriers 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. eu-LISAand the air carriers shall keep the logs that they created pursuant to paragraphs 1 and 2, respectively, for a time period of one year from the moment of the creation of those logs. They shall immediately and permanently delete those logs upon the expiry of that time period.

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

Article 14

Actions in case of technical impossibility to use the router

1. Where it is technically impossible to use the router to transmit API data because of a failure of the router, eu-LISA shall immediately notify the air carriers and 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 those parties when it has been successfully addressed.

During the time period between those notifications, Article 6(1) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) and Article 8(1) shall not apply either to the API data in question during that time period.

2. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 20 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 those parties when it has been successfully addressed.

During the time period between those notifications, Article 6(1) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) and Article 8(1) shall not apply either to the API data in question during that time period.

3. Where it is technically impossible to use the router to transmit API data because of a failure of the systems or infrastructure referred to in Article 21 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 those parties when it has been successfully addressed.

During the time period between those notifications, Article 6(1) shall not apply, insofar as the technical impossibility prevents the transfer of API data to the router. Insofar as that is the case, Article 4(1) and Article 8(1) shall not apply either to the API data in question during that time period.

When the technical impossibility has been successfully addressed, the air carrier concerned shall, without delay, submit to the competent national supervisory authority referred to in Article 29 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

Article 15

Personal data controllers

The competent border authorities shall be controllers, within the meaning of Article 4, point (7), of Regulation (EU) 2016/679, in relation to the processing of API data constituting personal data through the router , including the transmission and the storage for technical reasons of that data in the router, as well as in relation to their processing of API data constituting personal data referred to in Article 7 of this Regulation.

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

Article 16

Personal data processor

eu-LISA shall be the processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the processing of API data constituting personal data through the router in accordance with this Regulation and Regulation (EU) [API law enforcement].

Article 17

Security

1. eu-LISA shall ensure the security of the API data, in particular API data constituting personal data, that it processes pursuant to this Regulation and Regulation (EU) [API law enforcement]. 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. In particular, eu-LISA shall take the necessary measures 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 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 it is possible to verify and establish to which competent border authorities or PIUs the API data is transmitted through the router;

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

   (e) 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 33 of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/679.

Article 18

Self-monitoring

The air carriers and competent authorities shall monitor their compliance with their respective obligations under this Regulation, in particular as regards their processing of API data constituting personal data, including through frequent verification of the logs referred to in Article 13.

Article 19

Personal data protection audits

1. The competent national data protection authorities referred to in Article 51 of Regulation (EU) 2016/679 shall ensure that an audit of processing operations of API

data constituting personal data performed by the competent border autorities for the purposes of this Regulation is carried out, in accordance with relevant international auditing standards, at least once every four years.

2. The European Data Protection Supervisor shall ensure that an audit of processing operations of API data constituting personal data performed by eu-LISA for the purposes of this Regulation and Regulation (EU) [API law enforcement] is carried out 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, 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 13(1), and shall allow the European Data Protection Supervisor access to all eu-LISA's premises at any time.

CHAPTER 5

CONNECTIONS AND ADDITIONAL PROVISIONS REGARDING THE ROUTER

Article 20

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 of API data transferred purpsuant 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 is empowered to adopt delegated acts in accordance with Article 37 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 21

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 that 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.

2. The Commission is empowered to adopt delegated acts in accordance with Article 37 to supplement this Regulation by laying down the necessary detailed rules on the connections to and integration with the router referred to in paragraph 1.

Article 22

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 the 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 Regulation (EU) [API law enforcement], and that the router starts operations as soon as possible after the adoption by the Commission of the delegated acts provided for in Article 5(4), Article 6(3), Article 11(4), Article 20(2) and Article 21(2).

4. 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, PIUs and other relevant Member States' authorities and air carriers and inform the Commission of the outcome of that test.

Article 23

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 and Regulation (EU) [API law enforcement].

   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, Regulation (EU) [API law enforcement], 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, PIUs and air carriers.

3. eu-LISA shall not have access to any of the API data that is transmited through the router. However, that prohibition shall not preclude eu-LISA from having such access insofar as strictly necessary for the maintenance of the router.

4. Without prejudice to paragraph 3 of this Article and to Article 17 of Council Regulation (EEC, Euratom, ECSC) No 259/68[50], 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 24

eu-LISA's support tasks relating to the router

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

2. eu-LISA shall provide support to the competent border authorities and PIUs regarding the reception of API data through the router pursuant to this Regulation and Regulation (EU) [API law enforcement], respectively, in particular as regards the application of Articles 11 and 20 of this Regulation and Articles 5 and 10 of Regulation (EU) [API law enforcement].

Article 25

Costs of eu-LISA and of Member States

1. Costs incurred by eu-LISA in relation to the design, development, hosting and technical management of the router under this Regulation and Regulation (EU) [API law enforcement] shall be borne by the general budget of the Union.

2. Costs incurred by Member States in relation to their connections to and integration with the router referred to in Article 20 shall be borne by the general budget of the Union.

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

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

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

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

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

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

[50] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

Article 26

Liability regarding the router

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

Article 27

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 22(4). That implementing act shall be adopted in accordance with the examination procedure referred to in Article 36(2).

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

Article 28

Voluntary use of the router in application of Directive 2004/81/EC

1. Air carriers shall be entitled to use the router to transmit the information referred to in Article 3(1) of Directive 2004/82/EC to one or more of the responsible authorities referred to therein, in accordance with that Directive, provided that the responsible authority concerned has agreed with such use, from an appropriate date set by that authority. That authority shall only agree after having established that, in particular as regards both its own 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, it shall continue using the router to transmit such information to the responsible authority concerned until the date of application of this Regulation referred to in Article 39, second subparagraph. However, that use shall be discontinued, from an appropriate date set by that authority, where that authority considers that there are objective reasons that require such discontinuation and has informed the air carrier accordingly.

3. The responsible authority 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 6

SUPERVISION, PENALTIES, STATISTICS AND HANDBOOK

Article 29

National supervisory authority

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

2. Member States shall ensure that the national supervisory authorities have all necessary means and all necessary investigative and enforcement powers to carry out their tasks under this Regulation, including by imposing the penalties referred to in Article 30 where appropriate. They shall lay down detailed rules on the performance of those tasks and the exercise of those powers, ensuring that the performance and exercise is effective, proportionate and dissuasive and is subject to safeguards in compliance with the fundamental rights guaranteed under Union law.

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

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

Article 30

Penalties

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.

Member States shall, by the date of application of this Regulation referred to in Article 39, second subparagraph, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Article 31

Statistics

1. Every quarter, eu-LISA shall publish statistics on the functioning of the router, showing in particular the number, the nationality and the country of departure of the travellers, and specifically of the travellers who boarded the aircraft with inaccurate, incomplete or no longer up-to-date API data, with a non-recognised travel document, without a valid visa, without a valid travel authorization, or reported as overstay, the number and nationality of travellers.

2. eu-LISA shall store the daily statistics in the central repository for reporting and statistics established in Article 39 of Regulation (EU) 2019/817.

3. At the end of each year, eu-LISA shall compile statistical data in an annual report for that 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 supervisory authorities referred to in Article 29.

4. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of this Regulation and Regulation (EU) [API Law enforcement] as well as the statistics pursuant to paragraph 3.

5. eu-LISA shall have the right to access the following API data transmitted through to the router, solely for the purposes of the reporting referred to in Article 38 and for generating statistics in accordance with the present Article, without however such access allowing for the identification of the travellers concerned:

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

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

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

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

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

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

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

6. For the the purposes of the reporting referred to in Article 38 and for generating statistics in accordance with the present Article, eu-LISA shall store the data referred to in paragraph 5 of this Article in the central repository for reporting and statistics established by Article 39 of Regulation (EU) 2019/817. The cross-system statistical data and analytical reporting referred to in Article 39(1) of that Regulation shall allow the competent border authorities and other relevant authorities of the Member States to obtain customisable reports and statistics, for the purposes referred to in Article 1 of this Regulation.

7. The procedures put in place by eu-LISA to monitor the development and the functioning of the router referred to in Article 39(1) of Regulation (EU) 2019/817 shall include the possibility to produce regular statistics to ensure that monitoring.

Article 32

Practical handbook

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

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

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

CHAPTER 7

RELATIONSHIP TO OTHER EXISTING INSTRUMENTS

Article 33

Repeal of Directive 2004/82/EC

Directive 2004/82/EC is repealed from the date of application of this Regulation, referred to in Article 39, second subparagraph.

Article 34

Amendments to Regulation (EU) 2018/1726

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

(1) the following Article 13b is inserted:

"Article 13b

Tasks related to the router

In relation to Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*] and Regulation (EU) [API LE], the Agency shall perform the tasks related to the router conferred on it by those Regulations.

_____

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

(1) 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) and Articles 3 to 9 and Articles 11, [13a] and 13b 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."

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

(a) the following point (eeb) is inserted:

"(eeb) adopt reports on the state of play of the development of the router pursuant to Article 38(2) of the Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*];"

_____

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

(b) point (ff) is replaced by the following:

"(ff) adopt reports on the technical functioning of the following:

(1) SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council* and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council**;

(2) VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA;

(3) EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;

(4) ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;

(5) ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816;

(6) the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817, Article 74(3) of Regulation (EU) 2019/818 and of the router pursuant to Article 79(5) of Regulation (EU) …/… of the European Parliament and of the Council* [Prüm II Regulation] and Article 38(5) of Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*];

(3) the e-CODEX system pursuant to Article 16(1) of Regulation (EU) 2022/850"

_____

*Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

**Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(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 60(1) of the Regulation (EU) …/… of the European Parliament and of the Council* [Prüm II] and Article 19(3) of the Regulation (EU) …/… of the European Parliament and of the Council* *[this Regulation]* and ensure appropriate follow-up of those audits;

_____

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

Article 35

Amendments to Regulation (EU) 2019/817

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

"1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the 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) …/… of the European Parliament and of the Council* [*this Regulation*]."

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

2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 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 31(1) of Regulation (EU) …/… * [*this Regulation*]. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 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 38(2) of Regulation (EU) …/… [*this Regulation*]."

CHAPTER 8

FINAL PROVISIONS

Article 36

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), the third subparagraph, of Regulation (EU) No 182/2011 shall apply.

Article 37

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(4), Article 6(3), Article 11(4), Article 20(2) and Article 21(2) shall be conferred on the Commission for a period of five years from [*date of adoption of the Regulation*]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 5(4), Article 6(3), Article 11(4), Article 20(2) and Article 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

Article 38

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 [*one year after the date of entry into force of this Regulation*] and every year thereafter during the development phase of the router, eu-LISA shall produce a report, and submit it to the European Parliament and to the Council on the state of play of the development of the router. That 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 25.

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 as well as justifying any divergences.

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

   (a) the application of this Regulation;

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

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

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, including information not constituting personal data related to the results of the pre-checks of Union information systems and national databases at the external borders with API data. However, Member States may refrain from providing such information if, and to the extent necessary not to disclose confidential working methods or jeopardise ongoing investigations of the competent border authorities. The Commission shall ensure that any confidential information provided is appropriately protected.

Article 39

Entry into force and application

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

It shall apply from two years from the date at which the router starts operations, specified by the Commission in accordance with Article 27.

However:

(a) Article 5(4) and (5), Article 6(3), Article 11(4), Article 20(2), Article 21(2), Article 22, Article 25(1), Article 27, Article 36 and Article 37 shall apply from *[Date of entry into force of this Regulation]*;

(b) Article 10, Article 13(1), (3) and (4), Article 15, Article 16, Article 17, Article 23, Article 24, Article 26 and Article 28 shall apply from the date at which the router starts operations, specified by the Commission in accordance with Article 27.

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

Done at Strasbourg,

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

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

1. FRAMEWORK OF THE PROPOSALS

1.1. Title of the proposals

1. Regulation of the European Parliament and the Council on the collection and transfer of advance passenger information (API) for facilitating external border controls

2. Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

1.2. Policy area(s) concerned

Home affairs

1.3. The proposal/initiative relates to:

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[51]

☒ **the extension of an existing action**

☐ **a merger or redirection of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

1. Enhance external borders management and combating illegal immigration by ensuring that every person crossing the relevant external borders by air undergoes similar and necessary checks prior to entering.

2. Enhance the EU's internal security by ensuring that Member State's law enforcement authorities have access though their national Passenger Information Units to air traveller data that is necessary to prevent, detect and investigate serious crime and terrorism.

1.4.2. Specific objective(s)

Specific objective N°1: To enhance pre-checks at the relevant external borders with high quality and complete API data and facilitate the flow of travellers (on all inbound flights covered, including charter and business aviation).

Specific objective N°2: To prevent, detect and investigate serious crime and terrorism. with API data complementing PNR data on all inbound and outbound extra-EU flights and selected intra-EU flights.

To achieve specific objectives N°1 and N°2, the proposal includes the creation of a central API router.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The entry into the Union of **all airline travellers,** regardless of their nationality, is facilitated and accelerated by more efficient border checks based on the outcome of

[51] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

the systematic pre-checks performed on the way to the airport. Their check-in will be facilitated by the automated reading of travel document information.

eu-LISA will set up and operate a central API router as soon as possible from the date of adoption of both legal proposals.

A**ir carriers,** especially the ones exclusively operating intra-EU flights will have to make investments so as to provide API data to the router (EUR 75 million[52]) However for the overal air industry, those costs will be compensated by the rationalized and centralized approach to transmitting the information to competent national authorities. For instance, the delivery of API data to border authorities and Passenger Information units (PIU) via a single window, will substantially lower the number of connections, hence limiting the the operating costs (EUR +12,545 million per year instead of +40,3 million) and reduce the penalties usually imposed from poor or missing travel data (EUR 80 million per year).

Airports will gain from shorter border crossing times, indirectly reducing the need for landhold, and make transfers more reliable (hub)

The main beneficiaries are **law enforcement authorities, (Passenger Information Units) and the national border management authorities**. Mutualized data gathering will be less costly on the long run (EUR 20 million per year). The systematic and consistent approach will help make a more efficient use of resources for border checks at the airports. Available and accurate traveller data will help Passenger Information Units to keep track more reliably and efficiently of the movement of known suspects, and identify suspicious travel patterns of unknown individuals who may be involved in serious criminal or terrorist activities.

Citizens will directly and indirectly benefit from facilitated travel and entry to the Schengen area, as well as better crime fighting and lower crime rate. They are the true beneficiaries this initiative, helping to increase their protection.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Implementation of the central router :

– entry into operation date (as will be forecast and reported on a regular basis by eu-LISA Management Board) (target T0+5 years)

Specific objective N°1 :

– Share of airlines connected to the central router, operating extra-Schengen routes (target 100%)

– Number of national border management authorities receiving information from the central router

– Number of direct connections between airlines and national border management authorities for API (target 0)

[52] As per Impact Assessment

– Ratio: Number of API datasets transmitted directly to national border management authorities/ Number of API datasets transmitted to the router (target 0%)

– Share of flights where API datasets were received by the national border management authorities (target 100%)

– Share of flights where API datasets were received by the national border management authorities less than 30 minutes after take-off (100%)

– Number and amount of fines imposed to airlines for boarding a traveller on the basis of a travel document which machine readable data is unauthentic (target 0)

– Number and amount of fines imposed to airlines for inaccurate or incomplete datasets (target 0).

– Number and amount of fines imposed to airlines for lacking datasets (target 0.)

– Share of API datasets with complete identity data set (100%)

– Share of API datasets syntactically correct (100%)

– Number of travellers pre-checked on inbound flights covered: (same number as inbound travellers)

– Share of hits detected at the border that were already detected during pre-checks for inbound flights covered: target 100%

Specific objective n°2 :

– Share of airlines connected to the carrier interface/central router operating intra EU routes (target 100%)

– Number of PIUs connected to the central router (target 26)

– Number of direct connections between airlines and PIU for API (target 0)

– Ratio : Number of API datasets transmitted directly to PIU/ Number of API datasets transmitted to the router (target 0%)

– Share of PNR data received with corresponding API data (target 100%)

– Number of automated matches and hits (with PNR data only, with API data only, with both PNR and API)

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

Both initiatives require the development, followed by maintenance and operations of a central router (“the API router”), with two transitional periods. A/ Design and Development The design phase encompasses the router, the technical components needed to operate the router and the tools supporting together eu-LISA, air carriers and Member States in the implementation of their respective obligations.

It depends on (i) the adoption of the proposed Regulations (ii) the delivery of the technical components the router and the carrier interface that are dependent on (iii) the expected end of other development projects within eu-LISA which would relieve human resources that could be reassigned for other positions and tasks.

Assumptions are made that the legislative proposals are sent to the co-legislators by the end of 2022, and that the adoption process will be completed by the end of 2023, by analogy with the time taken for other proposals. The start of the development period is set at the end of 2025 (=T0) in order to have a reference point from where durations are counted, and not absolute dates. If adoption by co-legislators occurs at a later date, the whole schedule shifts accordingly. The development period is expected to be completed under those conditions by the end of 2028 (T0 + 3yrs.)

B/ Operation

Operation start and hence depend on the router and carrier interface entry into operations. (T1=T0 +3 years)

C/ Transitional period

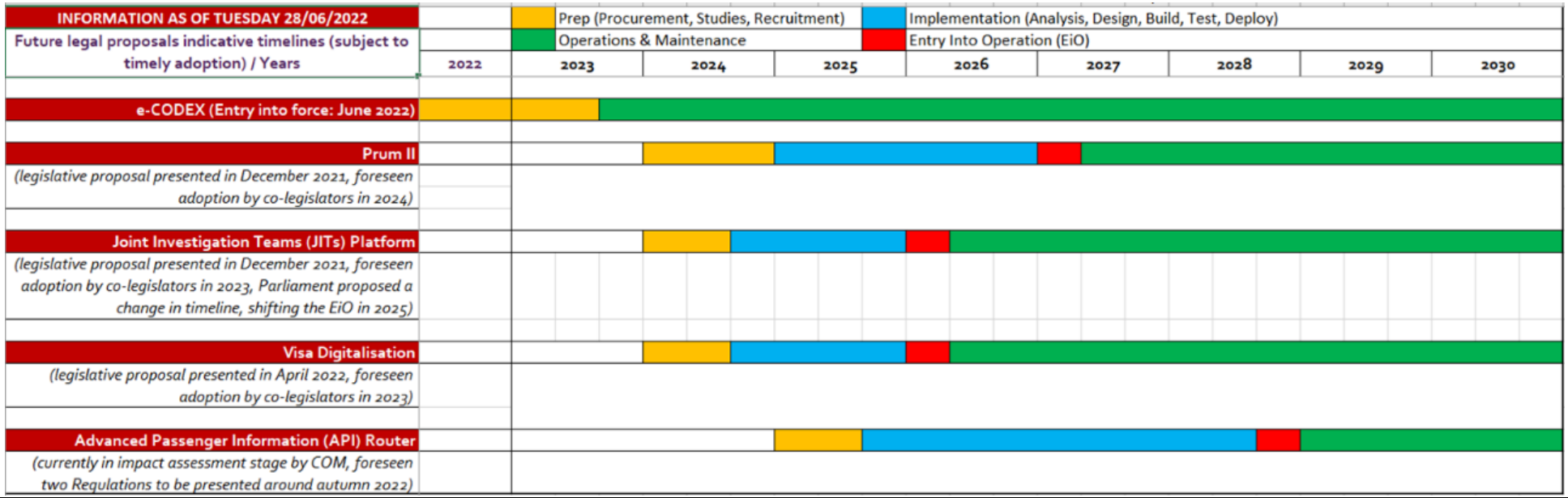
The transitional period depends on the router and carrier interface entry into operations, and allows for a progressive implementation by both, air carriers and Member States, of their respective obligations :

– for the air carriers: connection and transmission of API data to the carrier interface, systematic collection of data by automated means;

– for the Member States: collection of API data through the router.

This period should end 2 years after the entry into operations of the router and the carrier interface: (T1+2 years)

Timeline


INFORMATION AS OF TUESDAY 28/06/2022
Prep (Procurement, Studies, Recruitment)
Implementation (Analysis, Design, Build, Test, Deploy)
Operations & Maintenance
Entry Into Operation (EiO)
Future legal proposals indicative timelines (subject to timely adoption) / Years
2022
2023
2024
2025
2026
2027
2028
2029
2030
e-CODEX (Entry into force: June 2022)
Prum II
(legislative proposal presented in December 2021, foreseen adoption by co-legislators in 2024)
Joint Investigation Teams (JITs) Platform
(legislative proposal presented in December 2021, foreseen adoption by co-legislators in 2023, Parliament proposed a change in timeline, shifting the EiO in 2025)
Visa Digitalisation
(legislative proposal presented in April 2022, foreseen adoption by co-legislators in 2023)
Advanced Passenger Information (API) Router
(currently in impact assessment stage by COM, foreseen two Regulations to be presented around autumn 2022)

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante)

The Treaty on the Functioning of the European Union (TFEU) explicitly empowers the Union to develop a common policy on the checks to which persons crossing external borders are subject to, which is a clear objective to be pursued at EU level and on combating illegal immigation. At the same time, these are areas of shared competence between the EU and the Member States.

The impact assessment accompanying the proposal showed that (i) not every person crossing the external borders to reach the Union is pre-checked with API data and (ii) some gaps remain in the data collected for PNR purposes when API data is missing, which is especially true for intra-EU flights. EU action here aims at solving those issues, which can be taken in application of the principle of subsidiarity, relevant in this matter of shared competence, since the objectives envisaged cannot be achieved sufficiently by Member States alone and can be better achieved by the EU, by reason of the scale or effects of the proposed action:

(i) Member States alone would not be able to effectively implement clear and common operation rules on the processing of API data for border management and combating illegal immigration, especially on pre-checks, which are key to a harmonized approach across the Union and, in particular, the Schengen area to the movement of people across the external borders (Schengen Borders Code).

(ii) Likewise, Member States alone would not be able to effectively tackle the problems related to the processing of API data for law enforcement purposes, since the API Directive is a Schengen instrument and does not regulate the capture and transmission of API data on intra-EU flights. In the absence of API data that would complement the PNR data for these flights, Member States have implemented a variety of different measures that seek to compensate the lack of identity data on the travellers. This includes physical conformity checks to verify identity data between travel document and boarding card that generate new issues, without solving the underlying problem of not having API data.

Action at EU level on API data would therefore be required to address effectively the problems identified in accordance with the principle of subsidiarity. This is also called for in the June 2021 Commission's Strategy towards a fully functioning and resilient Schengen area[53] for an increased use of API data in combination with PNR data for intra-EU flights to significantly enhance internal security. In addition to the need to reinforce the Schengen area as a political priority of the Union, the need for EU action on API at this point in time, and notwithstanding the particular position of Ireland, also stems from recent legislative developments on Union's external border management:

– The 2019 Interoperability Regulations will enable systematic checks of persons crossing the Schengen external borders against all available information in EU centralised information systems for security, border and migration management.

[53] COM(2021) 277 final (2.6.2021).

Establishing a centralised transmission of API data at EU level is a logical continuation of this concept.

– At the Schengen external borders, the use of API data would effectively complement the imminent start of operation of the Entry Exit System (EES) and of the European Travel Information Authorisation System (ETIAS). The use of API data would remain necessary for the external borders management, as it informs border guards in advance whether a traveller has effectively boarded a plane from a third country and is about to enter the Schengen area, thus facilitating the border checks that will take place once that traveller arrives at the external border.

Expected Union added value to be generated (ex-post)

- Air carriers should benefit from technical, operational, infrastructure and administrative costs savings by drastically reducing the number of connections, exchange formats, procedures and messages sent to the Member States border management authorities and to the Passenger Information Units (theoretically divided by 26), despite an overall increase of the volume of passengers and flights concerned by the initiative.

- Harmonized rules on data collection for API data should have indirect impacts on police cooperation volume and quality, hence improving the **resolution of cross-border crime cases linked to the air vector** : PIU to PIU exchanges might expand on the basis that partner PIU have more chance to find appropriate information on their counterpart, (systematic collection) or know well in advance the chances to have it available (selective rules on data collection based on risk assessment according to harmonized rules)

- Reducing the remaining information gaps on scattered operators (business aviation, charters) or travellers that were still not concened by any check (crew), would help prevent, detect, and reduce traffic (drug trafficking and trafficking on human beings) that took advantage of such immune vectors.

1.5.3. Lessons learned from similar experiences in the past

Experience with the development of IT systems in the domain of Justice and Home Affairs, based on data exchange with third parties (e.g. air carriers), either as primary goal in a decentralized approach (API or PNR Directives,) or on an ancillary basis but centrally, such as EES and ETIAS (carrier gateway), allowed to identify the following lessons:

1. Implementation of a new regulation imposing new obligations to air carriers can be challenging: the somewhat scattered landscape involving many small actors, can lead to a lack of awareness and a slow uptake. Full implementation of API and PNR up to the “last percent” of air carriers can be difficult, even more so where traveller information is to be collected from business aviation and charter flights. Communication campaigns along with coordination with eu-LISA and the Member states authorities would be key to reach the full target.

In addition, experience with the deployment of centralized EU information systems on the field needing an adaptation or extension of national systems (VIS, SIS) proved that:

2. The implementation of the central component may suffer from cost overruns and delays that can come from changing requirements, due to the lack of underlying legal instruments setting out its purpose, scope, functions and technical specifications.

Hence the **preparatory design phase should wait for the legal instrument and its implementing and delegated acts readiness.**

2. As for the deployment of the system to the field, at national level, a progressive approach with incremental functional levels (SIS recast) is the most fit for implementing increasingly complex functional sets, and can both central and national developmeents to mature by reducing the focus on the quality assurance, increases the stability of the deliverables, crucial when multiple national systems have to be tested against the central system (availability of stable testing environement). A progressive approach starting with a few sites and reaching an increasing number of sites in a timely manner helps Member States manage the load on the procurement workstream, evens up the strain on financial resources and on logistical chain. It helps processing the feedback from the field on a limited set of pilot sites instead of exposing to massive unmanageable flow of some negative feedbacks. Lessons learned from pilot sites can benefit to the further massive deployment by feeding a training strategy. The central system, gains from a progressive ramp up the processing and the infrastructure and adapt if needed. Finally a progressive approach based on risk criteria linked to geographical factors (VIS) helps focus, for instance on the most complex businness situtions, helping finalzing the full functional spectrum of both central and national systems. Hence a **progressive approach based either on transitional phases, pilots, incremental functional steps and/or incremental geographical rollout should be favoured**.

3. It may be difficult to have an overview of the level of advancement in some Member States (initial SIS, VIS), namely the ones that had not provided for the respective activities in their multiannual programming or lacked precision in their programming. For EES, ETIAS and interoperability, a reimbursement mechanism of integration costs of Member State was foreseen and helped keep track of the implementation effort. **Therefore provisions for getting a more reliable picture on the level of integration of each Member State should be sought after.**

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The investments required at EU level and Member States level can be financed during the 2021-2027 multiannual financial framework (MFF) for the HOME Affairs Funds, by making use of the Internal Security Fund (ISF) and of the Instrument for Financial Support for Border Management and Visa Policy (BMVI), as part of the Integrated Border Management Fund. Funding beyond the year 2027 will fall within the negotiations of the next MFF.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The appropriations needed to finance the development of the API router by eu-LISA (EUR 34.967 million) have not been planned under the 2021-2027 MFF allocations for eu-LISA, as well as for DG HOME (EUR 2.653), as this is a new proposal for which amounts were not known at the time when the 2021-2027 MFF was tabled. Therefore, it is proposed to reinforce the eu-LISA budget and the DG HOME budget for the amounts needed in 2024, 2025, 2026 and 2027, by reducing the corresponding thematic facilities of the Border Management and Visa Policy Instrument (BMVI).

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☒ **unlimited duration**

– Implementation with a start-up period from 2024 to 2028,

– followed by full-scale operation as from 2029

1.7. Management mode(s) planned[54]

☐ **Direct management** by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☒ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☒ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

The design and development phase of the API router is expected to last four years during which eu-LISA will develop the components. The API router will be operational in the end of 2028.

[54] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

Shared management:

Each Member State shall establish a management and control systems for its programme and ensure the quality and the reliability of the monitoring system and of data on indicators, in accordance with the Common Provision Regulation[55] (CPR). The Member States shall send each year an assurance package, which includes the annual accounts, the management declaration and the audit authority's opinions on the accounts, the management and control system and the legality and regularity of the expenditure declared in the annual accounts. This assurance package will be used by the Commission to determine the amount chargeable to the Fund/Instrument for the accounting year. A review meeting between the Commission and each Member State shall be organised every two years to examine the performance of each programmes. The Member States send 6 times per year data for each programme, broken down by specific objectives. These data refers to the cost of operations and the values of common output and result indicators.

For the HOME Affairs Funds, the Member States will send an annual performance report, which should set out information on the progress in the implementation of their programmes and in achieving the milestones and targets. It should also raise any issues affecting the performance of the programme and describe the action taken to address them.

Under 2021-2027 HOME Affairs Funds, each Member States shall submit a final performance report. The final report should focus on the progress made towards achieving the objectives of the programme and should give an overview of the key issues that affected the programme's performance, the measures taken to address those issues and the assessment of the effectiveness of these measures. In addition, it should present the contribution of the programme to tackling the challenges identified in the relevant EU recommendations addressed to the Member State, the progress made in achieving the targets set out in the performance framework, the findings of the relevant evaluations and the follow-up given to those findings and the results of the communication actions.

Indirect management

The monitoring and reporting of the proposal will follow the principles outlined in eu-LISA's Regulation, the EU Financial Regulation and in line with the Common Approach on decentralised agencies. eu-LISA must notably send each year to the Commission, the European Parliament and the Council a Single Programming Document containing multi-annual and annual work programmes and resources programming. This Document sets out the objectives, expected results and performance indicators to monitor the achievement of the objectives and the results.

[55] Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy

eu-LISA must also submit a Consolidated Annual Activity Report to the management board. This report notably includes information on the achievement of the objectives and results set out in the Single Programming Document. The report must also be sent to the Commission, the European Parliament and the Council.

Moreover, as outlined in Article 39 of eu-LISA's Regulation, by 12 December 2023, and every five years thereafter, the Commission, after consulting the Management Board, shall evaluate, in accordance with the Commission's guidelines, the performance of the Agency in relation to its objectives, mandate, locations and tasks. That evaluation shall also include an examination of the implementation of this Regulation and the way and extent to which the Agency effectively contributes to the operational management of large-scale IT systems and to the establishment of a coordinated, cost-effective and coherent IT environment at Union level in the area of freedom, security and justice. That evaluation shall, in particular, assess the possible need to modify the mandate of the Agency and the financial implications of any such modification. The Management Board may issue recommendations regarding amendments to this Regulation to the Commission.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Shared management

For 2021-2027 period, the Regulation (EU) 2021/1148 of the European Parliament and of the Council of 7 July 2021 establishing, as part of the Integrated Border Management Fund, the Instrument for Financial Support for Border Management and Visa Policy and Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund will be managed for the first time under the CPR (Common Provision Regulation) rules.

For the shared management, the CPR builds on the management and control strategy in place for the 2014-2020 programming period, and introduces some measures aimed at simplifying the implementation and reducing the control burden at the level of both beneficiaries and Member States.

The novelties include:

- the removal of the designation procedure (which should allow to speed up the implementation of the programmes)

- management verifications (administrative and on-the-spot) to be carried out by the managing authority on a risk-basis (compared to the 100% administrative controls required in the 2014-2020 programming period). Furthermore, under certain conditions, the managing authorities may apply proportionate control arrangements in line with the national procedures.

- conditions to avoid multiple audits on the same operation/expenditure

The programme authorities will submit to the Commission interim payment claims based on expenditure incurred by beneficiaries. The CPR allows the managing authorities to carry out management verifications on a risk-basis and provides also for specific controls (e.g. on-the-spot controls by the managing authority and audits of operations/expenditure by the audit authority) after the associated expenditure has been declared to the Commission in the interim payment claims (up to 6 per year). In order to mitigate the risk of reimbursing ineligible expenditure, the CPR lays down

the Commission's interim payments to be capped at 95% of the amounts included in the payment application, given that initially only part of the national controls have been carried out. The Commission will pay the remaining balance following the annual clearance of accounts exercise, upon receipt of the assurance package from the programme management authorities. Any irregularities detected by the Commission or the European Court of Auditors after the transmission of the annual assurance package may lead to a net financial corrections.

Indirect management

Part of the proposal will be implemented via eu-LISA budget, through indirect management.

Pursuant to the principle of sound financial management, the budget of eu-LISA shall be implemented in compliance with effective and efficient internal control. eu-LISA is therefore bound to implement an appropriate control strategy coordinated among appropriate actors involved in the control chain.

Regarding ex-post controls, eu-LISA, as a decentralised agency, is notably subject to:

- internal audit by the Internal Audit Service of the Commission;

- annual reports by the European Court of Auditors, giving a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions;

- annual discharge granted by the European Parliament;

- possible investigations conducted by OLAF to ensure, in particular, that the resources allocated to agencies are put to proper use.

As partner DG to eu-LISA, DG HOME will implement its Control Strategy on decentralised agencies to ensure reliable reporting in the framework of its Annual Activity Report (AAR). While decentralised agencies have full responsibility for the implementation of their budget, DG HOME is responsible for regular payment of annual contributions established by the EU Budgetary Authorities.

Finally, the European Ombudsman provides a further layer of control and accountability at eu-LISA.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

No specific risks have been identified at this stage.

For the part management under shared management, the general risks in relation to the implementation of the current programmes concerns the under-implementation of the Fund/Instrument by the Member States and the possible errors derived from the complexity of rules and weaknesses in management and control systems. The draft CPR simplifies the regulatory framework by harmonising the rules and management and control systems across the different Funds implemented under shared management. It simplifies also the control requirements (e.g. risk-based management verifications, possibility for proportionate control arrangements based on national procedures, limitations of audit work in terms of timing and/or specific operations)

For the budget implemented by eu-LISA, a specific Internal Control Framework based on the Internal Control Framework of the European Commission is required.

The Single Programming Document must provide information on the internal control systems, while the Consolidated Annual Activity Report (CAAR) must contain information on the efficiency and effectiveness of the internal control systems, including as regards risk assessment. The CAAR 2021 reports that, the management of the Agency was reasonably confident that, overall, suitable controls are in place and that they are functioning as intended. Additionally, risks were being monitored and mitigated appropriately, and various improvements and reinforcements are implemented as necessary.

Another level of internal supervision is also provided by eu-LISA's Internal Audit Capability, on the basis of an annual audit plan notably taking into consideration the assessment of risks in eu-LISA. The Internal Audit Capability helps eu-LISA in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate the effectiveness of risk management, control, and governance processes, and by issuing recommendations for their improvement.

Moreover, the European Data Protection Supervisor and eu-LISA's data protection officer (an independent function attached directly to the Management Board Secretariat) supervise eu-LISA's processing of personal data.

Finally, as partner DG of eu-LISA, DG HOME runs an annual risk management exercise to identify and assess potential high risks related to agencies' operations, including eu-LISA. Risks considered as critical are reported annually in DG HOME management plan and are accompanied by an action plan stating the mitigating actions envisaged.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

For the shared management part, the cost of controls is expected to remain stable or potentially be reduced for the Member States.

There will be efficiency gains in implementation of the 2021-2027 HOME Affairs Funds programmes and increase in the payments to Member States.

With the risk based approach to management and controls being introduced in the applicable CPR to the HOME Affairs Funds, coupled with enhanced drive to adopt simplified cost options (SCOs), the cost of controls for Member States is expected to be further reduced.

For eu-LISA, the ratio of "control costs/value of the related funds managed" is reported on by the Commission. The 2021 AAR of DG HOME reports 0.08% for this ratio in relation to Indirect Management Entrusted Entities and Decentralised Agencies, including eu-LISA.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

DG HOME will continue to apply its Anti-Fraud Strategy in line with the Commission's Anti-Fraud Strategy (CAFS) in order to ensure inter alia that its internal anti-fraud related controls are fully aligned with the CAFS and that its fraud risk management approach is geared to identify fraud risk areas and adequate responses.

As regards shared management, Member States shall ensure the legality and regularity of expenditure included in the accounts submitted to the Commission. In this context, Member States shall take all required actions to prevent, detect and correct irregularities. Building on the past cycle 2014-2020, for 2021-2027 programming period as well, Member States are obliged to put in place procedures for detection of irregularities and anti-fraud coupled with the specific Commission Delegated Regulation on reporting of irregularities. Anti-fraud measures will remain a cross-cutting principle and obligation for Member States.

For indirect management, the measures related to combating fraud, corruption and any other illegal activities are outlined, inter alia, in article 50 of eu-LISA's Regulation and under Title X of eu-LISA's Financial Regulation.

eu-LISA shall notably participate in fraud prevention activities of the European Anti-fraud Office and inform the Commission without delay on cases of presumed fraud and other financial irregularities – in line with its internal anti-fraud strategy , revised and adopted in August 2022 covering period 2022-2024.

Moreover, as partner DG, in October 2021, DG HOME adopted a new Anti-Fraud Strategy, together with an accompanying Action Plan, which further strengthening the DG's anti-fraud capacities and adapting them to a constantly evolving environment. It takes into account the novelties introduced by the 2019 Commission Anti-Fraud Strategy and the adjustments required by the MFF 2021-2027.

Decentralised agencies, including eu-LISA, fall within the scope of the strategy. DG HOME 2021 AAR concluded that the fraud prevention and detection processes worked satisfactorily and therefore contributed to the assurance on the achievement of the internal control objectives.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[56]	from EFTA countries [57]	from candidate countries[58]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
4	11 02 01 Instrument for financial support for border management and visa policy	Diff.	NO	NO	YES	NO
4	11.01.01 – Support expenditure for the "Integrated Border Management Fund (IBMF) — Instrument for financial support for Border Management and Visa Policy (BMVI)	Non-Diff.	NO	NO	YES	NO
4	11 10 02 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA')	Non-Diff.	NO	NO	YES	NO
5	12 02 01 Internal Security Fund (ISF)	Diff.	NO	NO	NO	NO
5	11.02.02– Support expenditure for the Internal Security Fund (ISF) — Instrument for financial support for Border Management and Visa Policy (BMVI)	Non-Diff.	NO	NO	NO	NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	[XX.YY.YY.YY]		YES/NO	YES/NO	YES/NO	YES/NO

56 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
57 EFTA: European Free Trade Association.
58 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☒ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	4	Migration and Border Management

DG HOME			Year **2024**	Year **2025**	Year **2026**	Year **2027**	*Total* ***21-27***	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	*Total 28-34*	**TOTAL**
• Operational appropriations																
11 02 01 Instrument for financial support for border management and visa policy (BMVI)	Commitments	(1a)				8,250	*8,250*	7,838	9,075	10,313	5,363	5,363	5,363	5,363	*48,675*	**56,925**
	Payments	(2a)				2,888	*2,888*	4,393	6,394	8,642	7,734	7,219	6,538	5,610	*46,530*	**49,418**
11 10 02 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA')	Commitments	(1b)	0,157	2,597	7,958	22,865	*33,577*	15,415	9,168	9,083	9,083	9,083	9,083	9,083	*69,998*	**103,575**
	Payments	(2b)	0,157	2,597	7,958	22,865	*33,577*	15,415	9,168	9,083	9,083	9,083	9,083	9,083	*69,998*	**103,575**
Appropriations of an administrative nature financed from the envelope of specific programmes[59]																
Budget line		(3)														
TOTAL appropriations for DG HOME	Commitments	=1a+1b +3	0,314	3,993	7,958	31,115	*41,827*	23,253	18,243	19,396	14,446	14,446	14,446	14,446	*118,673*	**160,500**
	Payments	=2a+2b +3	0,314	3,993	7,958	25,753	*36,464*	19,808	15,562	17,725	16,817	16,302	15,621	14,693	*116,528*	**152,992**

[59] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL operational appropriations	Commitments	(4)	0,314	3,993	7,958	31,115	*41,827*	23,253	18,243	19,396	14,446	14,446	14,446	14,446	*118,673*	**160,500**
	Payments	(5)	0,314	3,993	7,958	25,753	*36,464*	19,808	15,562	17,725	16,817	16,302	15,621	14,693	*116,528*	**152,992**
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)														
TOTAL appropriations under HEADING 4 of the multiannual financial framework	Commitments	=4+ 6	0,314	3,993	7,958	31,115	*41,827*	23,253	18,243	19,396	14,446	14,446	14,446	14,446	*118,673*	**160,500**
	Payments	=5+ 6	0,314	3,993	7,958	25,753	*36,464*	19,808	15,562	17,725	16,817	16,302	15,621	14,693	*116,528*	**152,992**

Heading of multiannual financial framework	5	Security and Defence

DG HOME			Year **2024**	Year **2025**	Year **2026**	Year **2027**	*Total* ***21-27***	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	*Total 28-34*	**TOTAL**
• Operational appropriations																
12 02 01 Internal Security Fund (ISF)	Commitments	(1a)				3,300	*3,300*	3,135	3,630	4,125	2,145	2,145	2,145	2,145	19,470	**22,770**
	Payments	(2a)				1,155	*1,155*	1,757	2,558	3,457	3,094	2,888	2,615	2,244	18,612	**19,767**
Appropriations of an administrative nature financed from the envelope of specific programmes[60]																
Budget line		(3)														
TOTAL appropriations for DG HOME	Commitments	=1a+1b +3				3,300	*3,300*	3,135	3,630	4,125	2,145	2,145	2,145	2,145	*19,470*	**22,770**
	Payments	=2a+2b+3				1,155	*1,155*	1,757	2,558	3,457	3,094	2,888	2,615	2,244	*18,612*	**19,767**

[60] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL operational appropriations	Commitments	(4)				3,300	*3,300*	3,135	3,630	4,125	2,145	2,145	2,145	2,145	*19,470*	**22,770**
	Payments	(5)				1,155	*1,155*	1,757	2,558	3,457	3,094	2,888	2,615	2,244	*18,612*	**19,767**
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)														
TOTAL appropriations under HEADING 5 of the multiannual financial framework	Commitments	=4+ 6				3,300	*3,300*	3,135	3,630	4,125	2,145	2,145	2,145	2,145	*19,470*	**22,770**
	Payments	=5+ 6				1,155	*1,155*	1,757	2,558	3,457	3,094	2,888	2,615	2,244	*18,612*	**19,767**

• TOTAL operational appropriations (all operational headings)	Commitments	(4)	0,157	2,597	7,958	34,415	*45,127*	31,668	31,113	36,721	33,751	33,751	33,751	27,151	*227,903*	**273,030**
	Payments	(5)	0,157	2,597	7,958	26,908	*37,619*	23,413	22,409	28,706	31,461	33,379	34,208	31,589	*205,166*	**242,785**
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)														
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	0,157	2,597	7,958	34,415	*45,127*	26,388	21,873	23,521	16,591	16,591	16,591	16,591	*138,143*	**183,270**
	Payments	=5+ 6	0,157	2,597	7,958	26,908	*37,619*	21,565	18,119	21,182	19,911	19,189	18,236	16,937	*135,140*	**172,759**

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2024**	Year **2025**	Year **2026**	Year **2027**	***Total 21-27***	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	*Total 28-34*	**TOTAL**
DG HOME															
• Human resources		0,314	0,471	0,471	0,471	*1,727*	0,471	0,471	0,471	0,471	0,471	0,471	0,471	*3,297*	**5,024**
• Other administrative expenditure		0,187	0,273	0,273	0,273	*1,006*	0,273	0,273	0,273	0,187	0,187	0,187	0,187	1,488	**2,492**
TOTAL DG HOME	Appropriations	0,501	0,744	0,744	0,744	2,732	0,744	0,744	0,666	0,658	0,658	0,658	0,658	*4,785*	**7,516**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	0,501	0,744	0,744	0,744	2,732	0,744	0,744	0,666	0,658	0,658	0,658	0,658	*4,785*	**7,516**

EUR million (to three decimal places)

		Year **2024**	Year **2025**	Year **2026**	Year **2027**	*Total 21-27*	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	*Total 28-34*	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	0,815	4,737	8,702	35,159	47,858	27,131	22,617	24,186	17,249	17,249	17,249	17,249	*142,928*	**190,786**
	Payments	0,815	4,737	8,702	27,651	40,351	22,309	18,863	21,847	20,569	19,847	18,894	17,595	*139,925*	**180,275**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2024**		Year **2025**		Year **2026**		Year **2027**		Year **2028**		Year **2029**		Year **2030**		Year **2031**		Year **2032**		Year **2033**		Year **2034**			
	Type[61]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	**Total cost**
COMMON OBJECTIVE																										
- Build Router		44,482	0,004	0,157	0,058	2,597	0,179	7,958	0,507	22,565	0,252	11,205													1	**44,482**
Operate router		9,083								0,300		4,210		9,168		9,083		9,083		9,083		9,083		9,083		**59,093**
Subtotal for common objective				0,157		2,597		7,958		22,865		15,415		9,168		9,083		9,083		9,083		9,083		9,083		**103,575**
SPECIFIC OBJECTIVE No 1																										
- Build MS connection	26	1,031							8	8,250	6	6,188	6	6,188	6	6,188									26	**26,813**
- Maintain MS connection	26	0.206									8	1,650	14	2,888	20	4,125	26	5,363	26	5,363	26	5,363	26	5,363	26	**30,113**
Subtotal for specific objective n°1										8,250		7,838		9,075		10,313		5,363		5,363		5,363		5,363		**56,925**
SPECIFIC OBJECTIVE No 2																										
- MS connection	26	0,413							8	3,300	6	2,475	6	2,475	6	2,475									26	**10,725**
- Maintain MS connection	26	0.083									8	0,660	14	1,155	20	1,650	26	2,145	26	2,145	26	2,145	26	2,145	26	**12,045**
Subtotal for specific objective n°2				0,000		0,000		0,000		3,300		3,135		3,630		4,125		2,145		2,145		2,145		2,145		**22,770**
TOTALS				**0,157**		**2,597**		**7,958**		**34,415**		**26,388**		**21,873**		**23,521**		**16,591**		**16,591**		**16,591**		**16,591**		**183,270**

[61] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

3.2.3. Estimated impact on eu-LISA's human resources

3.2.3.1. Summary

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Temporary agents (AD Grades)	0,157	1,099	2,198	2,355	4,710	2,355	2,355	2,355	2,355	2,355	2,355
Temporary agents (AST grades)											
Contract staff	0,000	0,298	0,680	0,850	1,955	1,105	1,020	1,020	1,020	1,020	1,020
Seconded National Experts											
TOTAL	**0,157**	**1,397**	**2,878**	**3,205**	**6,665**	**3,460**	**3,375**	**3,375**	**3,375**	**3,375**	**3,375**

Staff requirements (FTE):

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Temporary agents (AD Grades)	2,0	14,0	14,0	15,0	30,0	15,0	15,0	15,0	15,0	15,0	15,0
Temporary agents (AST grades)											
Contract staff	0,0	7,0	8,0	10,0	23,0	13,0	12,0	12,0	12,0	12,0	12,0
Seconded National Experts											
TOTAL	**2,0**	**21,0**	**22,0**	**25,0**	**53,0**	**28,0**	**27,0**	**27,0**	**27,0**	**27,0**	**27,0**

Staff from eu-LISA should be supporting DG HOME efforts in elaborating the secondary legislation early in 2024, therefore staff shall be operational as soon as possible. Recruitment procedures shall start as of January 2024. A 50% factor is applied for 2 FTE recruited in 2024, 21 FTE in 2025. The rest of the staff comes from the redeployment from other projects.

3.2.4. Summary of estimated impact on administrative appropriations (for DG HOME)

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	Total **21-27**	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	*Total **28-34***	**TOTAL**
HEADING 7 of the multiannual financial framework														
Human resources	0,314	0,471	0,471	0,471	1,727	0,471	0,471	0,471	0,471	0,471	0,471	0,471	*3,297*	**5,024**
Other administrative expenditure	0,187	0,273	0,273	0,273	1,006	0,273	0,273	0,273	0,187	0,187	0,187	0,187	1,567	**2,573**
Subtotal HEADING 7 of the multiannual financial framework	0,501	0,744	0,744	0,744	2,733	0,744	0,744	0,744	0,658	0,658	0,658	0,658	*4,864*	**7, 597**

Outside HEADING 7[62] of the multiannual financial framework														
Human resources														
Other expenditure of an administrative nature														
Subtotal outside HEADING 7 of the multiannual financial framework														

TOTAL	0,501	0,744	0,744	0,744	2,733	0,744	0,744	0,744	0,658	0,658	0,658	0,658	*4,864*	**7, 597**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

62 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.4.1. Estimated requirements of human resources (for DG HOME)

– ☐ The proposal/initiative does not require the use of human resources.

– ☒ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**
• Establishment plan posts (officials and temporary staff)									
20 01 02 01 (Headquarters and Commission's Representation Offices)	2	3	3	3	3	3	3	3	3
20 01 02 03 (Delegations)									
01 01 01 01 (Indirect research)									
01 01 01 11 (Direct research)									
Other budget lines (specify)									

External staff (in Full Time Equivalent unit: FTE)

20 02 01 (AC, END, INT from the 'global envelope')									
20 02 03 (AC, AL, END, INT and JPD in the delegations)									
XX 01 xx **yy zz** [63]	- at Headquarters								
	- in Delegations								
01 01 01 02 (AC, END, INT - Indirect research)									
01 01 01 12 (AC, END, INT - Direct research)									
Other budget lines (specify)									
TOTAL	**2**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	Three officials for the follow-up. The staff deal with taking up the Commission's duties in the delivery of the programme: checking compliance with legal proposal, addressing compliance issues, preparing reports to European Parliament and Council, assessing Member State progress, keeping secondary legislation up-to-date including any development concerning the standards. As the programme is an additional activity compared with existing workloads, additional staff is required (1 FTE).
External staff	

[63] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.5. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☒ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

As the appropriations required for the development of the API router (2024/2028) and recurring costs (as from 2029) have not been planned under the eu-LISA 2021-2027 MFF allocation, nor for DG HOME supplementary staff, the funding required, respectively for the development and maintenance of the API router (EUR 33.577 million under the 2021-2027 MFF) and for the Commission follow-up efforts (EUR 2.732 million) will be made available via bugdetary offsetting against BMVI (11.02.01 – 'Border Management and Visa Instrument') for the corresponding amounts:

Appropriations CA=PA million EUR : 2024 : 0.157 ; 2025 : 2.597, 2026 : 7.958; 2027 : 22.865

Representing 2024-2027 : 33.577

The development and recurring costs at national level should be financed under the succesor of the BMVI for the subsequent MFF.[64]

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– ☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.6. Third-party contributions

The proposal/initiative:

– ☒ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

[64] The budget impact beyond the current MFF is an indicative overview, without prejudice to the future MFF Agreement.

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has no financial impact on revenue.

– ☑ The proposal/initiative has the following financial impact:

(1) ☐ on own resources

(2) ☑ on other revenue

(3) please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[65]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….		p.m.						

For assigned revenue, specify the budget expenditure line(s) affected.

11.1002 (eu-LISA), 11.0201 (BMVI)

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

The budget shall include a contribution from countries associated with the implementation, application and development of the Schengen acquis and the visa digitalisation related measures as laid down in the respective agreements in force. The estimates shall be based on calculations for revenues for the implementation of the Schengen acquis from the States that currently contribute (Iceland, Norway and Switzerland) to the general budget of the European Union (consumed payments) an annual sum for the relevant financial year, calculated in accordance with its gross domestic product as a percentage of the gross domestic product of all the participating States. The calculation shall be based on figures from EUROSTAT which are subject to considerable variation depending on the economic situation of the participating States.

[65] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.