EUROPEAN
COMMISSION

Brussels, 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)

{SWD(2017) 473 final} - {SWD(2017) 474 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Background of the proposal

In the past three years, the EU has experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks. EU citizens expect external border controls on persons, and checks within the Schengen area, to be effective, to enable effective management of migration and to contribute to internal security. These challenges have brought into sharper focus the urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management, migration and security.

Information management in the EU can and must be made more effective and efficient, in full respect of fundamental rights including, in particular, the right to the protection of personal data, in order to better protect the EU's external borders, improve the management of migration and enhance internal security for the benefit of all citizens. There are already a number of information systems at EU level, and more systems are being developed, to provide border guards, immigration and law enforcement officers with relevant information on persons. For this support to be effective, the information provided by EU information systems needs to be complete, accurate and reliable. However, there are structural shortcomings in the EU information management architecture. National authorities face a complex landscape of differently governed information systems. Moreover, the architecture of data management for borders and security is fragmented, as information is stored separately in unconnected systems. This leads to blind spots. As a consequence, **the various information systems at EU level are currently not interoperable** — that is, able to exchange data and share information so that authorities and competent officials have the information they need, when and where they need it. Interoperability of EU-level information systems can significantly contribute to eliminating the current blind spots where persons, including those possibly involved in terrorist activities, can be recorded in different, unconnected databases under different aliases.

In April 2016, the Commission presented a **Communication *Stronger and smarter information systems for borders and security***[1] to address a number of structural shortcomings related to information systems.[2] The aim of the April 2016 Communication was to initiate a discussion on how information systems in the European Union can better enhance border and migration management and internal security. The **Council**, for its part, similarly recognised the urgent need for action in this area. In June 2016, it endorsed a **roadmap to enhance information exchange and information management** including interoperability solutions in the Justice and Home Affairs area.[3] The purpose of the roadmap was to support operational investigations and to swiftly provide front-line practitioners — such as police officers, border guards, public prosecutors, immigration officers and others — with comprehensive, topical and high-quality information to cooperate and act effectively. The **European Parliament** has

[1] COM(2016) 205 of 6 April 2016. .

[2] (1) Sub-optimal functionalities in some of the existing information systems; (2) information gaps in the EU's architecture of data management; (3) a complex landscape of differently governed information systems; and (4) a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots.

[3] Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

also urged action in this area. In its July 2016 Resolution[4] on the Commission's work programme for 2017, the European Parliament called for '*proposals to improve and develop existing information systems, address information gaps and move towards interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by necessary data protection safeguards*'. President Juncker's State of the Union address in September 2016[5] and the European Council conclusions of December 2016[6] highlighted the importance of overcoming the current shortcomings in data management and of improving the interoperability of existing information systems.

In June 2016, as a follow-up to the April 2016 Communication, the Commission set up a **high-level expert group on information systems and interoperability**[7] in order to address the legal, technical and operational challenges of enhancing interoperability between central EU systems for borders and security, including their necessity, technical feasibility, proportionality and data protection implications. The **final report** of the high-level expert group was published in May 2017.[8] It set out a range of recommendations to strengthen and develop the EU's information systems and their interoperability. The EU Agency for Fundamental Rights, the European Data Protection Supervisor and the EU Counter-Terrorism Coordinator all participated actively in the work of the expert group. Each submitted supportive statements, while acknowledging that wider issues on fundamental rights and data protection had to be addressed in moving forward. Representatives of the Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and of the General Secretariat of the Council attended as observers. The high-level expert group concluded that it is **necessary and technically feasible to work towards practical solutions for interoperability** and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements.

Building on the expert group's report and recommendations, the Commission set out, in the *Seventh progress report towards an effective and genuine Security Union*,[9] a **new approach to the management of data** for borders, security and migration management where all centralised EU information systems for security, border and migration management are interoperable in full respect of fundamental rights. The Commission announced its intention to pursue work towards creating a European search portal capable of querying simultaneously all relevant EU systems in the areas of security, border and migration management, possibly with more streamlined rules for law enforcement access, and to develop for these systems a shared biometric matching service (possibly with a hit-flagging functionality[10]) and a common identity repository. It announced its intention to present, as soon as possible, a legislative proposal on interoperability.

---

4 European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP)).

5 State of the Union 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_en.

6 European Council conclusions (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability — 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

10 New privacy-by-design concept that restricts the access to all data by limiting it to a mere 'hit/no-hit' notification, indicating the presence (or non-presence) of data.

The European Council conclusions of June 2017[11] reiterated the need to act. Building on the June 2017 conclusions[12] of the Justice and Home Affairs Council, the European Council invited the Commission to prepare, as soon as possible, draft legislation enacting the recommendations made by the high-level expert group. This initiative also responds to the Council's call for a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs[13]. In order to reinforce the efforts to make the European Union a safer society, in full compliance with fundamental rights, the Commission announced, in the context of its 2018 Work Programme[14], a proposal on the interoperability of information systems to be presented by the end of 2017.

- **Objectives of the proposal**

The general objectives of this initiative result from the Treaty-based goals of improving the management of the Schengen external borders and contributing to the internal security of the European Union. They also stem from policy decisions by the Commission and relevant (European) Council Conclusions. These objectives are further elaborated in the European Agenda on Migration and subsequent communications, including the Communication on preserving and strengthening Schengen,[15] the European Agenda on Security[16] and the Commission's work and progress reports towards an effective and genuine Security Union.[17]

Whilst building in particular on the April 2016 Communication and the findings of the high-level expert group, the objectives of this proposal are intrinsically linked to the above.

The specific objectives of this proposal are to:

(1) ensure that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have **fast, seamless, systematic and controlled access** to the information that they need to perform their tasks;

(2) provide a solution to **detect multiple identities** linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of *bona fide* persons and **combating identity fraud**;

(3) facilitate **identity checks of third-country nationals**, on the territory of a Member State, by police authorities; and

(4) facilitate and **streamline access by law enforcement authorities** to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.

---

11 European Council conclusions, 22-23 June 2017.

12 Outcomes of the 3546th Council meeting on Justice and Home Affairs on 8 and 9 June 2017, 10136/17.

13 The Council's Committee of Permanent Representatives (Coreper), upon giving the mandate to the Council Presidency to start interinstitutional negotiations on the EU Entry/Exit System on 2 March 2017, agreed a draft Council statement calling on the Commission to propose a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs (Summary Record 7177/17, 21.3.2017).

14 COM(2017) 650 final.

15 COM(2017)570 final.

16 COM(2015)185 final.

17 COM(2016)230 final.

In addition to these primary operational objectives, this proposal will also contribute to:

- facilitating the technical and operational **implementation by Member States** of existing and future new information systems;
- strengthening and streamlining the **data security and data protection conditions** that govern the respective systems; and
- improving and harmonising **data quality** requirements of the respective systems.

Finally, this proposal includes provisions for the establishment and governance of the Universal Message Format (UMF) as an EU standard for the development of information systems in the area of justice and home affairs, and the establishment of a central repository for reporting and statistics.

- **Scope of the proposal**

Together with its sister proposal presented the same day, this interoperability proposal focuses on the EU information systems for security, border and migration management that are operated at the central level, three of them existing, one on the brink of development, and two others at the stage of proposals under discussion between co-legislators. Each system has its own objectives, purposes, legal bases, rules, user groups and institutional context.

The three existing centralised information systems so far are:

- the **Schengen Information System (SIS)** with a broad spectrum of alerts on persons (refusals of entry or stay, EU arrest warrant, missing persons, judicial procedure assistance, discreet and specific checks) and objects (including lost, stolen and invalidated identity or travel documents);[18]
- the **Eurodac** system with fingerprint data of asylum applicants and third-country nationals who have crossed the external borders irregularly or who are illegally staying in a Member State; and
- the **Visa Information System (VIS)** with data on short-stay visas.

In addition to these existing systems, the Commission proposed in 2016-2017 three new centralised EU information systems:

- the **Entry/Exit System (EES)**, for which the legal basis has just been agreed, which will replace the current system of manual stamping of passports and will electronically register the name, type of travel document, biometrics and the date and place of entry and exit of third-country nationals visiting the Schengen area for a short stay;
- the proposed **European Travel Information and Authorisation System (ETIAS)**, which would, once adopted, be a largely automated system that would gather and verify information submitted by visa-exempt third-country nationals ahead of their travel to the Schengen area; and

[18] The Commission's December 2016 draft Regulations on SIS propose to further extend this to include return decisions and inquiry checks.

- the proposed **European Criminal Record Information System for third-country nationals (ECRIS-TCN system)**, which would be an electronic system for exchanging information on previous convictions handed down against third-country nationals by criminal courts in the EU.

These six systems are complementary and — with the exception of the Schengen Information System (SIS) — exclusively focused on third-country nationals. The systems support national authorities in managing borders, migration, visa processing and asylum, and in fighting crime and terrorism. The latter applies in particular to the SIS, which is the most widely used law enforcement information-sharing instrument today.

In addition to these information systems, centrally managed at EU level, the scope of this proposal also includes **Interpol**'s Stolen and Lost Travel Documents (SLTD) database, which pursuant to the provisions of the Schengen Borders Code is systematically queried at the EU's external borders, and Interpol's Travel Documents Associated with Notices (TDAWN) database. It also covers **Europol** data, as far as this is relevant for the functioning of the proposed ETIAS system and for assisting Member States when querying data on serious crime and terrorism.

National information systems and decentralised EU information systems are outside the scope of this initiative. Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework,[19] the Passenger Name Record (PNR) Directive[20] and the Advance Passenger Information Directive[21] may at a later stage be linked up to one or more of the components proposed under this initiative.[22]

To respect the distinction between the matters which constitute a development of the Schengen acquis regarding borders and visa on the one hand and other systems which concern the Schengen acquis on police cooperation or are not related to the Schengen acquis on the other, this proposal deals with access to the Schengen Information System as currently regulated by Council Decision 2007/533/JHA as well as with Eurodac and [ECRIS-TCN].

- **The necessary technical components to achieve interoperability**

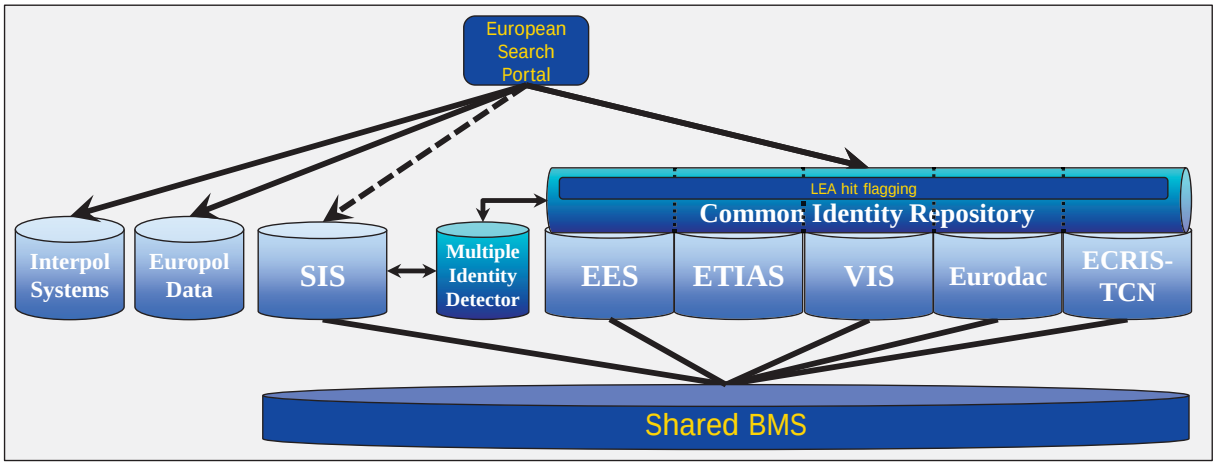
In order to achieve the objectives of this proposal, four interoperability components need to be established:

- European search portal — ESP
- Shared biometric matching service — shared BMS
- Common identity repository — CIR
- Multiple-identity detector — MID

Each of these components is described in detail in the Commission Staff Working Document on the impact assessment accompanying this proposal.

The four components combined lead to the following interoperability solution:

[19] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.
[20] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.
[21] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.
[22] Similarly as regards the customs systems, the Council in its June 2017 conclusions invited the Commission to undertake a feasibility study to further explore the technical, operational and legal aspects of interoperability of the security and border management systems with customs systems, and present its findings for discussion by the Council by the end of 2018.



The objectives and functioning of these four components can be summarised as follows:

(1) The **European search portal (ESP)** is the component that would enable the simultaneous query of multiple systems (Central-SIS, Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN systems, as well as the relevant Interpol systems and Europol data) using identity data (both biographical and biometric). It would ensure that users of the EU information systems have fast, seamless, efficient, systematic and controlled access to all information that they need to perform their tasks.

A query through the European search portal would immediately, in a matter of seconds, return information from the various systems to which the user has legal access. Depending on the purpose of the query, and the corresponding access rights, the ESP would be provided with specific configurations.

The ESP does not process any new data, and it does not store any data; it would act as a single window or 'message broker' to query various central systems and retrieve the necessary information seamlessly, and would do so in full respect of the access control and data protection requirements of the underlying systems. The ESP would facilitate the correct and authorised use of each of the existing EU information systems, and would make it easier and cheaper for Member States to consult and use the systems, in line with the legal instruments that govern these systems.

(2) The **shared biometric matching service (shared BMS)** would enable the querying and comparison of biometric data (fingerprints and facial images) from several central systems (in particular, SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system). The proposed ETIAS will not contain biometric data and would therefore not be linked to the shared BMS.

Where each existing central system (SIS, Eurodac, VIS) currently has a dedicated, proprietary search engine for biometric data[23], a shared biometric matching service would provide a common platform where the data is queried and compared simultaneously. The shared BMS would generate substantial benefits in terms of security, cost, maintenance and operation by relying on one unique technological component instead of five different

[23] These biometric search engines are technically referred to as automated fingerprint identification system (AFIS) or automated biometric identification system (ABIS).

ones. The biometric data (fingerprint and facial images) are exclusively retained by the underlying systems. The shared BMS would create and retain a mathematical representation of the biometric samples (a template) but would discard the actual data, which remains thus stored in one location, only once.

The shared BMS would be a key enabler to help detect connections between data sets and different identities assumed by the same person in different central systems. Without a shared BMS, none of the other three components will be able to function.

(3) The **common identity repository (CIR)** would be the shared component for storing biographical[24] and biometric identity data of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. Each of these five central systems records or will record biographical data on specific persons for specific reasons. This would not change. The relevant identity data would be stored in the CIR but would continue to 'belong' to the respective underlying systems that recorded this data.

The CIR would not contain SIS data. The complex technical architecture of SIS containing national copies, partial national copies and possible national biometric matching systems would make the CIR very complex to a degree where it may no longer be technically and financially feasible.

The key objective of the CIR is to facilitate the biographical identification of a third-country national. It would offer increased speed of operations, improved efficiency and economies of scale. The establishment of the CIR is necessary to enable effective identity checks of third-country nationals, including on the territory of a Member State. In addition, by adding a 'hit-flag functionality' to the CIR it would be possible to check the presence (or non-existence) of data in any of the systems covered by the CIR through a simple hit/no-hit notification. This way, the CIR would also help streamlining of access by law enforcement authorities to non-law enforcement information systems, while maintaining a high data protection safeguard (see the section on the two-step approach to law enforcement access, hereunder).

Out of the five systems to be covered by the CIR, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system are new systems that still need to be developed. The current Eurodac does not have biographical data; this extension will be developed once the new legal base for Eurodac is adopted. The current VIS does contain biographical data, but the necessary interactions between VIS and the future EES will require an upgrading of the existing VIS. The creation of the CIR therefore would arrive at the right moment. It would not in any way involve duplicating existing data. Technically, the CIR would be developed on the basis of the EES/ETIAS platform.

(4) The **multiple-identity detector (MID)** would check whether the queried identity data exists in more than one of the systems connected to it. The MID covers the systems that store identity data in the CIR (Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system) as well as the SIS. The MID would enable the detection of multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of *bona fide* persons and combating identity fraud.

[24] Biographical data that can be found on the travel document includes; last name, first name, gender, date of birth, travel document number. They do not include addresses, former names, biometric data, etc.

The MID would enable to establish that different names belong to the same identity. It is a necessary innovation to effectively address the fraudulent use of identities, which is a serious breach of security. The MID would only show those biographical identity records that have a link in different central systems. These links would be detected by using the shared biometric matching service on the basis of biometric data and would need to be confirmed or rejected by the authority that recorded the data in the information system that led to the creation of the link. To assist the authorised users of the MID in this task, the system would need to label the identified links in four categories:

- Yellow link - potentially differing biographical identities on the same person
- White link - confirmation that the different biographical identities belong to the same *bona fide* person
- Green link - confirmation that different *bona fide* persons happen to share the same biographic identity
- Red link - suspicion that different biographical identities are unlawfully used by the same person.

This proposal describes the procedures that would be put in place to handle these different categories. The identity of affected *bona fide* persons should be disambiguated as quickly as possible, by turning the yellow link into a confirmed green or white link, so as to ensure that no unnecessary inconveniences will be faced. Where, on the other hand, the assessment leads to the confirmation of a red link, or a change from a yellow into a red link, appropriate action would need to be taken.

- **The two-step approach to law enforcement access as provided by the common identity repository**

Law enforcement is defined as a secondary or ancillary objective of Eurodac, VIS, the future EES and the proposed ETIAS. As a result, the possibility of accessing data stored in these systems for the purpose of law enforcement is restricted. Law enforcement authorities can only consult directly these non-law enforcement information systems for the purpose of prevention, investigation, detection or prosecution of terrorism and other serious criminal offences. Moreover, the respective systems are governed by different access conditions and safeguards and some of those current rules could hinder the speed of the legitimate use of the systems by these authorities. More generally, the principle of prior search limits the possibility of Member State authorities to consult systems for justified law enforcement purposes and could thereby result in missed opportunities to uncover necessary information.

In its April 2016 Communication, the Commission acknowledged the need to optimise the existing tools for law enforcement purposes, whilst respecting data protection requirements. This necessity was confirmed and reiterated by Member States and relevant agencies in the framework of the high-level expert group.

In light of the above, by creating the CIR with a so-called 'hit-flag functionality', this proposal introduces the possibility for accessing the EES, the VIS, the ETIAS and Eurodac using a **two-step data consultation approach**. This two-step approach would not change the fact that law enforcement is a strictly ancillary objective of these systems and therefore needs to follow strict rules for access.

As a first step, a law enforcement officer would launch a query on a specific person using the person's identity data, travel document or biometric data to check whether information on the searched person is stored in the CIR. Where such data is present, the officer will receive **a reply indicating which EU information system(s) contains data** on this person (the **hit-flag**). The officer would not have actual access to any data in any of the underlying systems.

As a second step, the officer may individually request access to each system that has been indicated as containing data, in order to obtain the complete file on the queried person, **in line with the existing rules and procedures established by each system concerned**. This second step access would remain subject to prior authorisation by a designated authority and would continue to require a specific user ID and logging.

This new approach would also bring added value to law enforcement authorities due to the **existence of potential links** in the MID. The MID would help the CIR identifying existing links, which makes the search even more accurate. The MID would be able to indicate whether the person is **known under different identities** in different information systems.

The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence **is unknown**. Indeed, in those cases, the CIR would enable identifying the information system that knows the person in one single search. By doing so, the existing conditions of prior searches in national databases and of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA ('Prüm check') become redundant.

The new two-step consultation approach would only **enter into force once** the necessary interoperability **components are fully operational**.

- **Additional elements of this proposal to support the interoperability components**

(1) In addition to the above components, this draft Regulation also includes the proposal to establish a **central repository for reporting and statistics (CRRS)**. This repository is necessary to enable the creation and sharing of reports with (anonymous) statistical data for policy, operational and data quality purposes. The current practice of gathering statistical data only on the individual information systems is detrimental to data security and performance and it does not enable the correlating of data across systems.

The CRRS would provide a dedicated, separate repository for anonymous statistics extracted from SIS, VIS, Eurodac, the future EES, the proposed ETIAS, the proposed ECRIS-TCN system, the common identity repository, the multiple-identity detector and the shared biometric matching service. The repository would provide for the possibility of secured sharing of reports (as regulated by the respective legal instruments) to Member States, Commission (including Eurostat) and EU agencies.

Developing one central repository instead of separate repositories for each system would lead to a lower cost and less effort for its establishment, operations and maintenance. It would also bring a higher level of data security as data is stored and access control is managed in one repository.

(2) This draft Regulation also proposes to establish the **Universal Message Format (UMF)** as the standard that would be used at EU level to orchestrate interactions between multiple systems in an interoperable way, including the systems developed and managed by eu-LISA. The use of the standard by Europol and Interpol would also be encouraged.

The UMF standard introduces a common and unified technical language to describe and link data elements, in particular the elements relating to persons and (travel) documents. Using UMF when developing new information systems guarantees easier integration and interoperability with other systems, in particular for Member States needing to build interfaces to communicate with these new systems. In this respect, the compulsory use of UMF when developing new systems can be considered a necessary precondition for the introduction of the interoperability components proposed in this Regulation.

In order to ensure the complete roll-out across the EU of the UMF standard, an appropriate governance structure is proposed. The Commission would be responsible for establishing and developing the UMF standard, in the framework of an examination procedure with the Member States. Schengen associated states EU agencies and international bodies participating in the UMF projects (such as eu-LISA, Europol and Interpol) will also be involved. The proposed governance structure is vital for the UMF in order to extend and expand the standard while guaranteeing maximum usability and applicability.

(3) This draft Regulation furthermore introduces the concepts of **automated data quality control mechanisms** and common quality indicators, and the need for Member States to ensure the highest level of data quality when feeding and using the systems. If data is not of the highest quality, there can be consequences not just for not being able to identify wanted persons, but also by affecting the fundamental rights of innocent people. To overcome problems that can arise from the input of data by human operators, automatic validation rules can prevent operators from making mistakes. The goal would be to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions. This would be supplemented by regular data quality reports to be produced by the eu-LISA.

- **Consequences for other legal instruments**

Together with its sister proposal, this draft Regulation introduces innovations that will require amendments of other legal instruments:

- Regulation (EU) No 2016/399 (the Schengen Borders Code)
- Regulation (EU) 2017/2226 (the EES Regulation)
- Regulation (EC) No 767/2008 (the VIS Regulation)
- Council Decision 2004/512/EC (the VIS Decision)
- Council Decision 2008/633/JHA (the VIS/law enforcement access Decision)
- [the ETIAS Regulation]
- [the Eurodac Regulation]
- [the SIS Regulations]

- [the ECRIS-TCN Regulation, including the corresponding provisions of Regulation (EU) 2016/1624 (the European Border and Coast Guard Regulation)]
- [the eu-LISA Regulation]

This current proposal and its sister proposal include detailed provisions for the necessary changes to the legal instruments that are currently stable texts as adopted by the co-legislators: the Schengen Borders Code, the EES Regulation, the VIS Regulation, Council Decision 2008/633/JHA and Council Decision 2004/512/EC.

The other listed instruments (Regulations on ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) are currently under negotiation in the European Parliament and Council. For these instruments, it is therefore not possible to set out the necessary amendments at this stage. The Commission will present such amendments for each of these instruments within two weeks of a political agreement on the respective draft Regulations being reached.

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

This proposal comes within the framework of the broader process that was launched by the April 2016 Communication *Stronger and smarter information systems for borders and security*, and the subsequent work of the high-level expert group on information systems and interoperability. The aim is to pursue three objectives:

(a) strengthen and maximize the benefits of **existing information systems**;

(b) address information gaps by establishing new information systems;

(c) enhance interoperability between these systems.

On the first objective, the Commission adopted proposals in December 2016 for the further reinforcement of the existing Schengen Information System (SIS)[25]. On Eurodac, following the Commission's proposal of May 2016[26], negotiations on the revised legal basis were accelerated. A proposal for a new legal basis for the Visa Information System (VIS) is also under preparation, and will be submitted in the second quarter of 2018.

Regarding the second objective, negotiations on the Commission's April 2016 proposal to establish an Entry/Exit System (EES)[27] were concluded as early as July 2017, when the co-legislators reached a political agreement, confirmed by the European Parliament in October 2017 and formally adopted by the Council in November 2017. The legal base will enter into force in December 2017. Negotiations on the November 2016 proposal for the establishment of a European Travel Information and Authorisation System (ETIAS)[28] have started and are expected to be finalised in the coming months. In June 2017, the Commission proposed a legal basis for addressing another information gap: the European Criminal Record Information System for third-country nationals (ECRIS-TCN system)[29]. Here again, the co-legislators have indicated that they aim for an early adoption of this legal basis.

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.

This current proposal addresses the third objective identified in the April 2016 Communication.

- **Consistency with other Union policies in the area of Justice and Home Affairs**

This proposal together with its sister proposal delivers on, and is in line with, the European Agenda on Migration and subsequent communications, including the Communication on preserving and strengthening Schengen[30], as well as the European Agenda on Security[31] and the Commission's work and progress reports towards an effective and genuine Security Union[32]. It is consistent with other Union policies, in particular as follows:

- Internal security: the European Agenda on Security states that common high standards of border management are essential to prevent cross-border crime and terrorism. This proposal further contributes to achieving a high level of internal security by offering the means for authorities to have fast, seamless, systematic and controlled access to the information they require.
- Asylum: the proposal includes Eurodac as one of the central EU systems to be covered by interoperability.
- External border management and security: this proposal reinforces the SIS and VIS systems, which contribute to the efficient control of the Union's external borders, as well as the future EES and the proposed ETIAS and ECRIS-TCN system.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The main legal basis will be the following articles of the Treaty on the Functioning of the European Union: Article 16(2), Article 74, Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2).

Under Article 16(2), the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Under Article 74, the Council can adopt measures to ensure administrative cooperation between departments of the Member States in the area of justice, liberty and security. Under Article 78, the Union has the power to adopt measures for a common European asylum system. Under Article 79(2)(c), the Union has the power to adopt measures in the area of illegal immigration and unauthorised residence. Under Articles 82(1)(d) and 87(2)(a), the Union has the power to adopt measures to strengthen police and judicial cooperation concerning the collection, storage, processing, analysis and exchange of relevant information. Under Articles 85(1) and 88(2), the Union has the power to determine the tasks of Eurojust and Europol, respectively.

- **Subsidiarity**

Freedom of movement within the EU requires that the external borders of the Union are effectively managed to ensure security. Member States have therefore agreed to address these challenges collectively, especially by sharing information through centralised EU systems in

[30] COM(2017)570 final.
[31] COM(2015)185 final.
[32] COM(2016)230 final.

the area of justice and home affairs. This is confirmed by the various conclusions that have been adopted by both the European Council and the Council, especially since 2015.

The absence of internal border controls requires sound management of the Schengen external borders, where each Member State or Schengen associated country has to control the external border on behalf of the other Schengen states. Consequently, no Member State alone is able to cope on its own with irregular migration and cross-border crime. Third-country nationals who enter the area without internal border controls are able to travel freely within it. In an area without internal borders, action against irregular immigration and international crime and terrorism, including through the detection of identity fraud, should be undertaken in common, and can only be successfully addressed at EU level.

Key common information systems at EU level are in place or in the process of being put in place. Enhanced interoperability among these information systems necessarily entails EU-level action. At the heart of the proposal is the improved efficiency and use of centralised systems managed by eu-LISA. By reason of the scale, effects and impact of the envisaged actions, the fundamental objectives can only be achieved efficiently and systematically at EU level.

- **Proportionality**

As explained in full detail in the impact assessment accompanying this proposed Regulation, the policy choices made in this proposal are considered proportionate. They do not go beyond what it necessary to achieve the agreed objectives.

The **European search portal (ESP)** is a necessary tool to reinforce the authorised use of the existing and future EU information systems. The impact of the ESP in terms of data processing is very limited. It will not store any data, except information regarding the various user profiles of the ESP, and the data and information systems to which they have access, and keeping track of their use by means of logs. The role of the ESP as a message broker, an enabler and a facilitator, is proportionate, necessary and limited in terms of searches and access rights under the mandates of the legal bases dealing with information systems and the proposed Regulation on interoperability.

The **shared biometric matching service (shared BMS)** is necessary for the functioning of the ESP, the common identity repository and the multiple-identity detector and facilitates the use and maintenance of the existing and future relevant EU information systems. Its functionality enables the performing of searches on biometric data from various sources in an efficient, seamless and systematic way. The biometric data are stored and retained by the underlying systems. The shared BMS creates templates but will discard the actual images. The data is thus stored in one location, only once.

The **common identity repository (CIR)** is necessary in order to achieve the purpose of correct identification of a third-country national, e.g. during an identity check within the Schengen area. The CIR also supports the functioning of the multiple-identity detector and is therefore a necessary component to achieve the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. Access to the CIR for this purpose is limited to those users that need this information to carry out their tasks (which requires these checks to become a new ancillary purpose of Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system). The data processes are strictly limited to what is needed to achieve this goal, and adequate safeguards will be established to ensure access rights are respected and the data stored in the CIR is the minimum necessary. In order to

ensure data minimisation and to avoid unjustified duplication of data, the CIR holds the required biographic data of each of its underlying systems — stored, added, modified and deleted in accordance with their respective legal basis — without copying it. Data retention terms are fully aligned with the data retention provisions of the underlying information systems providing the identity data.

The **multiple-identity detector (MID)** is necessary to provide a solution for the detection of multiple identities with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The MID will contain the links between individuals present in more than one central information system, strictly limited to the data needed to verify that a person is recorded lawfully or unlawfully under different biographical identities in different systems but also to clarify that two persons having similar biographical data may not be the same person. Data processing through the MID and the shared BMS in order to link individual files across individual systems is kept to an absolute minimum. The MID will include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.

- **Choice of the instrument**

A Regulation of the European Parliament and the Council is proposed. The proposed legislation addresses directly the operation of central EU information systems for borders and security, all of which have been, or are proposed to be, established under Regulations. Similarly, eu-LISA, which will be responsible for the design and development, and in due course technical management, of the components is also established under a Regulation. A Regulation is therefore the appropriate choice of instrument.

3. RESULTS OF STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Public consultation**

In preparation of this proposal the Commission launched in July 2017 a public consultation to collect the views of interested stakeholders on the subject of interoperability. The consultation received 18 responses from a variety of stakeholders, including Member State governments, private sector organisations, other organisations such as NGOs and think tanks, as well as private citizens[33]. Overall, the responses were broadly in favour of the underlying principles of this interoperability proposal. The vast majority of respondents agreed that the issues the consultation identified were the correct ones, and that the objectives that the interoperability package seeks to achieve are correct. In particular, respondents considered that the options outlined in the consultation paper would:

- help staff on the ground access the information they need;
- avoid duplication of data, reduce overlaps and highlight discrepancies in data;
- identify people more reliably — including people with multiple identities — and reduce identity fraud.

A clear majority of respondents supported each of the proposed options and considered them to be necessary to achieve the objectives of this initiative, underlining in their responses the need for strong and clear data protection measures, particularly in relation to access to the

[33] Further details are contained in the synopsis report annexed to the impact assessment.

information stored in the systems and data retention, and the need for up-to-date, high-quality data in the systems and measures to ensure this.

All the points raised have been taken into account in the preparation of this proposal.

- **Eurobarometer survey**

In June 2017, a Special Eurobarometer[34] survey was conducted, showing that the EU's strategy of sharing information at EU level to combat crime and terrorism has widespread public support: almost all respondents (92 %) agree that national authorities should share information with the authorities of other Member States to better fight crime and terrorism.

A clear majority (69 %) of respondents expressed the view that the police and other national law enforcement authorities should share information with other EU countries on a systematic basis. In all Member States, a majority of respondents think that information should be shared in every case.

- **High-level expert group on information systems and interoperability**

As already indicated in the introduction, this current proposal builds on the recommendations of the **high-level expert group on information systems and interoperability**[35]. This group was established in June 2016 with the objective of addressing the legal, technical and operational challenges of available options to achieve interoperability between central EU systems for borders and security. The group took a broad and comprehensive perspective on the data management architecture for border management and law enforcement, taking into account also the relevant roles, responsibilities and systems for customs authorities.

The group comprised experts from Member States and Schengen associated countries, and from the EU agencies eu-LISA, Europol, the European Asylum Support Office, the European Border and Coast Guard Agency and the EU Agency for Fundamental Rights. The EU Counter-Terrorism Coordinator and the European Data Protection Supervisor also participated as full members of the expert group. In addition, representatives of the secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and of the General Secretariat of the Council attended as observers.

The **final report of the high-level expert group** was published in May 2017[36]. It underlined the need to act to address the structural shortcomings identified in the April 2016 Communication. It set out a range of recommendations to strengthen and develop the EU's information systems and interoperability. It concluded that it is **necessary and technically feasible to work towards the European search portal, the shared biometric matching service and the common identity repository as solutions for interoperability** and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements. The group also recommended considering the additional option of a two-step approach towards law enforcement access, based on a hit-flagging functionality.

---

[34] The *Report on Europeans' attitudes towards security* analyses the results of the Special Eurobarometer public opinion survey (464b) regarding citizens' overall awareness, experiences and perceptions of security. This survey was carried out by TNS Political & Social network in the 28 Member States between 13 and 26 June 2017. Some 28 093 EU citizens from different social and demographic categories were interviewed.

[35] Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability — 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

This draft Regulation also responds to the high-level experts group's recommendations on data quality, the Universal Message Format (UMF) and the establishment of a data warehouse (here presented as the central repository for reporting and statistics (CRRS)).

The fourth interoperability component proposed in this draft Regulation (the multiple-identity detector) was not identified by the high-level expert group, but arose during the course of additional technical analysis and the proportionality assessment conducted by the Commission.

- **Technical studies**

Three studies were commissioned to support the preparation of the proposal. Contracted by the Commission, Unisys delivered a report on a feasibility study for the European search portal. eu-LISA commissioned a technical report from Gartner (with Unisys) to support the development of the shared biometric matching service. PWC delivered to the Commission a technical report on a common identity repository.

- **Impact assessment**

This proposal is supported by an impact assessment as presented in the accompanying Staff Working Document SWD(2017) 473.

The Regulatory Scrutiny Board reviewed the draft impact assessment at its meeting of 6 December 2017 and delivered its opinion (positive with reservations) on 8 December indicating that the impact assessment be adjusted in order to integrate the Board's recommendations on specific aspects. These related firstly to additional measures under the preferred option streamlining end-users' existing data access rights in EU information systems, and to illustrate associated safeguards for data protection and fundamental rights. The second main consideration was to clarify the integration of the Schengen Information System under option 2, including effectiveness and costs to facilitate its comparison with the preferred option 3. The Commission updated its impact assessment to respond to these main considerations and to address a number of other comments made by the Board.

The impact assessment evaluated if and how each of the identified objectives could be achieved by using one or more of the technical components identified by the high-level expert group and through subsequent analysis. Where necessary it also looked into sub-options necessary to meet these objectives, whilst respecting the data protection framework. The impact assessment concluded that:

- To meet the objective of providing authorised users with fast, seamless, systematic and controlled access to relevant information systems, a European search portal (ESP) should be created, built on a shared biometric matching service (shared BMS) to address all databases.
- To meet the objective of facilitating identity checks of third-country nationals, on the territory of a Member State, by authorised officers, a common identity repository (CIR) should be created, containing the minimum set of identification data, and built on the same shared BMS.
- To meet the objective of detecting multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud, a multiple-identity detector (MID) should be built, containing links between multiple identities across systems.

- To meet the objective of facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems, for the purpose of preventing, investigating, detecting or prosecuting serious crime and terrorism, a 'hit-flag' functionality should be included in the CIR.

Since all objectives must be met, the **complete solution is the combination of ESP, CIR (with hit flagging) and MID, all relying on the shared BMS**.

The major positive impact will be the improvement of border management and increased internal security within the European Union. The new components will streamline and expedite access by national authorities to the necessary information and identification of third-country nationals. They will enable authorities to make cross-links to already existing, necessary information on individuals during border checks, for visa or asylum applications, and for police work. This will enable access to information that can support reliable decisions being made, whether relating to investigations of serious crime and terrorism or decisions in the field of migration and asylum. Whilst not directly affecting EU nationals (the proposed measures are primarily focused on third-country nationals whose data is recorded in an EU centralised information system), the proposals are expected to generate increased public trust by ensuring that their design and use increases the security of EU citizens.

The immediate financial and economic impacts of the proposal will be limited to the design, development and operation of the new facilities. The costs will fall to the EU budget and to Member State authorities operating the systems. The impact on tourism will be positive as the proposed measures will both improve the security of the European Union and should also be beneficial for a speedier border control. Similarly, the impact on airports, seaports and carriers is expected to be positive, in particular because of expedited border control checks.

- **Fundamental rights**

The impact assessment looked in particular into the impacts of the proposed measures on fundamental rights and, in particular, to the right to data protection.

In accordance with the Charter of Fundamental Rights of the EU, to which EU institutions and Member States, when they implement EU law, are bound (Article 51(1) of the Charter), the opportunities offered by interoperability as a measure to enhance security and the protection of the external border need to be balanced with the obligation to ensure that interferences with fundamental rights that may derive from the new interoperability environment are limited to what is strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality (Article 52(1) of the Charter).

The proposed interoperability solutions are complementary components to existing systems. As such, they would not alter the balance already ensured by each of the existing central systems as regards their positive impact on fundamental rights.

Nevertheless, interoperability does have the potential of having an additional, indirect impact on a number of fundamental rights. Indeed, the correct identification of a person has a positive impact on the right to respect for private life, and in particular the right to one's identity (Article 7 of the Charter), as it can contribute to avoid identity confusions. On the other hand, conducting checks based on biometric data can be perceived as interfering with the person's right to dignity (in particular, where it is perceived as humiliating) (Article 1). Yet in a

survey[37] by the EU Agency for Fundamental Rights, respondents were specifically asked whether they believed that giving their biometrics in the context of border control might be humiliating. The majority of respondents did not feel that it would.

The proposed interoperability components offer the opportunity to adopt targeted preventive measures to enhance security. As such, they can contribute to the protection of people's right to life (Article 2 of the Charter), which also implies a positive obligation on authorities to take preventive operational measures to protect an individual whose life is at risk, if they know or ought to have known of the existence of an immediate risk[38], as well as to uphold the prohibition of slavery and forced labour (Article 5).Through a reliable, more accessible and easier identification, interoperability can support the detection of missing children or children subject to people trafficking, and facilitate swift and targeted responses.

A reliable, more accessible and easier identification could also contribute to ensuring that the right to asylum (Article 18 of the Charter) and the prohibition of refoulement (Article 19 of the Charter) are effectively ensured. Interoperability could in fact prevent situations where asylum applicants are unlawfully apprehended, detained and made subject to undue expulsion. Furthermore, through interoperability, identity fraud will be more easily identified. It would also reduce the need to share data and information about asylum applicants with third countries (particularly the country of origin) for the purpose of establishing the person's identity and obtaining travel documents, which could potentially endanger the person concerned.

- **Protection of personal data**

Given the personal data involved, interoperability will especially have an impact on the right to the protection of personal data. This right is established by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union, and in Article 8 of the European Convention on Human Rights. As underlined by the Court of Justice of the EU[39], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[40]. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter.

According to the General Data Protection Regulation[41], the free movement of data within the EU is not to be restricted for reasons of data protection. However, a series of principles must be met. Indeed, to be lawful, any limitation on the exercise of the fundamental rights protected by the Charter must comply with the following criteria, laid down in its

---

37 *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders*, Report by the EU Agency for Fundamental Rights: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

38 European Court of Human Rights, Osman v United Kingdom, No. 87/1997/871/1083, 28 October 1998, para. 116.

39 Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

40 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.

41 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).

Article 52(1):

- it must be provided for by law;
- it must respect the essence of the rights;
- it must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;
- it must be necessary; and
- it must be proportional.

This current proposal embeds all these data protection rules, as set out in full detail in the impact assessment accompanying this proposed Regulation. The proposal is based on the principles of data protection by design and by default. It includes all appropriate provisions limiting data processing to what is necessary for the specific purpose and granting data access only to those entities that 'need to know'. Data retention periods (where relevant) are appropriate and limited. Access to data is reserved exclusively for duly authorised staff of the Member State authorities or EU bodies that are competent for the specific purposes of each information system and limited to the extent that the data are required for the performance of tasks in accordance with these purposes.

4. BUDGETARY IMPLICATIONS

The budgetary implications are included in the attached financial statement. It covers the remaining period of the current multiannual financial framework (until 2020) and the seven years of the following period (2021-2027). The proposed budget for the years 2021 and beyond is included for illustrative purposes and does not prejudge the next multiannual financial framework.

The implementation of this proposal will require budgetary allocations for:

(1) The **development** and integration by eu-LISA of the four interoperability components, and the central repository for reporting and statistics, and their subsequent **maintenance and operations**.

(2) The **data migration** to the shared biometric matching service (shared BMS) and the common identity repository (CIR). In the case of the shared BMS, the biometric templates of the corresponding data from the three systems that currently use biometrics (SIS, VIS and Eurodac) need to be recreated on the shared BMS. In the case of CIR, the personal data elements from VIS need to be migrated to the CIR, and the possible links found between identities in SIS, VIS and Eurodac need to be validated. This last process, in particular, is resource intensive.

(3) The update by eu-LISA of the **national uniform interface** (NUI) already included in the EES Regulation to become a generic component that allows the exchange of messages between Member States and the central system(s).

(4) The **integration of Member State national systems** with the NUI that will convey the messages exchanged with CIR/ multiple-identity detector through the European search portal.

(5) The **training** on the use of the interoperability components by end-users, including through the European Union Agency for Law Enforcement Training (CEPOL).

The interoperability components are built and maintained as a programme. While the European search portal (ESP) and the multiple-identity detector are entirely new components, along with the central repository for reporting and statistics (CRRS), the shared BMS and the CIR are shared components that combine existing data held (or to be held) in existing or new systems with their existing budgetary estimates.

The **ESP** will implement existing, known interfaces towards SIS, VIS and Eurodac and will in due course be extended towards new systems.

The ESP will be used by Member States and agencies using an interface based on Universal Message Format (UMF). This new interface will require developments, adaptations, integrations and testing by the Member States, eu-LISA, Europol and the European Border and Coast Guard Agency. The ESP would use the concepts of the national uniform interface (NUI) introduced for EES, which would lower the integration efforts.

The ESP will generate additional costs for Europol in order to make the QUEST interface available for use with basic protection level (BPL) data.

The basis of the **shared BMS** will *de facto* be established with the creation of the new EES as this constitutes by far the greatest volume of new biometric data. The required budget was reserved under the EES legal instrument. Adding further biometric data from VIS, SIS and Eurodac to the shared BMS constitutes an additional cost mainly linked to the migration of existing data. This is estimated at EUR 10 m for all three systems. Adding new biometric data from the proposed ECRIS-TCN system constitutes a limited additional cost that can be covered from the funds reserved under the proposed ECRIS-TCN legal instrument to establish an ECRIS-TCN automated fingerprint identification system.

The common identity repository will be established with the creation of the future EES and further extended when developing the proposed ETIAS. The storage and search engines for these data were included in the budget reserved under the future EES and the proposed ETIAS legal instruments. Adding new biographical data from both Eurodac and the proposed ECRIS-TCN system constitutes a minor additional cost that was already reserved under the Eurodac and the proposed ECRIS-TCN legal instruments.

The total budget required over nine years (2019-2027) amounts to EUR 424.7 million, covering the following items:

(1) A budget of EUR 225 million for eu-LISA which covers the total cost for the development of the programme delivering the five interoperability components (EUR 68.3 million), the maintenance cost from the moment components are delivered up until 2027 (EUR 56.1 million), a specific budget of EUR 25 million for the migration of data from existing systems to the shared BMS and the additional costs for the NUI update, network, training and meetings. A specific budget of EUR 18.7 million covers the cost of upgrading and operating ECRIS-TCN in high-availability mode from 2022.

(2) A budget of EUR 136.3 million for Member States to cover the changes to their national systems in order to use the interoperability components, the NUI delivered by eu-LISA and a budget for the training of the substantial end-user community.

(3) A budget of EUR 48.9 million for Europol to cover the upgrade of Europol's IT systems to the volume of messages to be handled and the increased performance

levels[42]. The interoperability components will be used by ETIAS in order to consult the Europol data.

(4) A budget of EUR 4.8 million for the European Border and Coast Guard Agency for hosting a team of specialists who during one year will validate the links between identities at the moment the multiple-identity detector goes live.

(5) A budget of EUR 2.0 million for European Union Agency for Law Enforcement Training (CEPOL) to cover the preparation and delivery of training to operational staff.

(6) A provision of EUR 7.7 million for DG HOME in order to cover a limited increase of staff and related costs during the development period of the different components, as the Commission will also have to fulfil additional tasks during that period and takes the responsibility for the committee dealing with Universal Message Format.

The Internal Security Fund (ISF) Borders Regulation is the financial instrument where the budget for the implementation of the interoperability initiative has been included. It provides in Article 5(b) that EUR 791 million is to be implemented through a programme for developing IT systems based on existing and/or new IT systems, supporting the management of migration flows across the external borders subject to the adoption of the relevant Union legislative acts and under the conditions laid down in Article 15(5). Of this EUR 791 million, EUR 480.2 million is reserved for the development of the EES, EUR 210 million for ETIAS and EUR 67.9 million for the revision of SIS. The remainder (EUR 32.9 million) is to be reallocated using ISF-B mechanisms. The current proposal requires EUR 32.1 million for the current multiannual financial framework period (2019/20) which therefore fits with the remaining budget.

5. ADDITIONAL INFORMATION

• Implementation plans and monitoring, evaluation and reporting arrangements

eu-LISA is responsible for the operational management of large-scale IT systems in the area of freedom, security and justice. As such, it is already entrusted with the operation and technical and operational improvements of existing systems, and the development of the future systems already envisaged. Under this proposed Regulation, it will define the design of the physical architecture of the interoperability components, develop and implement them, and ultimately host them. The respective components will be implemented incrementally, in conjunction with the development of the underlying systems.

The Commission will ensure that systems are in place to monitor the development and functioning of the four components (European search portal, shared biometric matching service, common identity repository, multiple-identity detector) and the central repository for reporting and statistics, and evaluate them against the main policy objectives. Four years after the functionalities are put in place and operating, and every four years thereafter, eu-LISA should submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components. In addition, five years after the functionalities are put in place and operating, and every four years thereafter, the Commission

[42] The current information handling capacity of Europol is not compliant with the substantial volumes (average of 100,000 queries per day) and shortened response time that will be required by ETIAS.

should produce an overall evaluation of the components, including on the direct or indirect impact of the components and of its practical implementation on fundamental rights. It should examine results achieved against objectives and assess the continuing validity of the underlying rationale and any implications for future options. The Commission should submit the evaluation reports to the European Parliament and the Council.

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

Chapter I sets out the general provisions for this Regulation. It explains: the principles underlying the Regulation; the components established therein; the objectives that interoperability seeks to address; the scope of this Regulation; the definitions of the terms used in this Regulation; and the principle of non-discrimination regarding the processing of data under this Regulation.

Chapter II sets out the provisions for the European search portal (ESP). This chapter provides for the establishment of the ESP and its technical architecture, to be developed by eu-LISA. It specifies the aim of the ESP and identifies those who may use the ESP and how they are to use it in accordance with existing access rights for each of the central systems. There is a provision for eu-LISA to create user profiles for each category of user. This chapter sets out how the ESP will query central systems and provides for the content and format of replies to users. Chapter II also provides that eu-LISA will keep logs of all processing operations, and provides for the fall-back procedure in case the ESP would be unable to access one or more of the central systems.

Chapter III sets out the provisions for the shared biometric matching service (shared BMS). This chapter provides for the establishment of the shared BMS and its technical architecture, to be developed by eu-LISA. It specifies the aim of the shared BMS and sets out what data it stores. It explains the relationship between the shared BMS and the other components. Chapter III also provides that the shared BMS will not continue to store data once the data is no longer contained in the respective central system and provides that eu-LISA will keep logs of all processing operations.

Chapter IV sets out the provisions for the common identity repository (CIR). This chapter provides for the establishment of the CIR and its technical architecture, to be developed by eu-LISA. It sets out the aim of the CIR and clarifies which data will be stored, and how, including provisions to ensure the quality of the data stored. This chapter provides that the CIR will create individual files based on data held in the central systems, and that individual files are updated in line with changes in the individual central systems. Chapter IV also specifies how the CIR will operate in relation to the multiple-identity detector. This chapter identifies those who may have access to the CIR and how they may access the data in accordance with access rights, and more specific provisions depending on whether access is for identification purposes or, as a first step of the two-step approach, for accessing the EES, the VIS, the ETIAS and Eurodac via the CIR for law enforcement purposes. Chapter IV also provides that eu-LISA will keep logs of all processing operations concerning the CIR.

Chapter V sets out the provisions for the multiple-identity detector (MID). This chapter provides for the establishment of the MID and its technical architecture, to be developed by eu-LISA. It explains the aim of the MID and regulates the use of the MID in accordance with access rights to each of the central systems. Chapter V sets out when and how the MID will launch searches to detect multiple identities, and how results are delivered and to be followed up, including when necessary through manual verification. Chapter V sets out a classification of the types of link that can result from the search depending on whether the result shows a single identity, multiple identities or shared identity data. This chapter provides that the MID

will store linked data held in the central systems while data remains in two or more individual central systems. Chapter V also provides that eu-LISA will keep logs of all processing operations concerning the MID.

Chapter VI makes provision for measures to support interoperability. It provides for improving data quality, establishing the Universal Message Format as the common standard for information exchange supporting interoperability, and creating a central repository for reporting and statistics.

Chapter VII relates to data protection. This chapter makes provisions ensuring that data processed under this Regulation is processed lawfully and appropriately, in line with the provisions of Regulation No 45/2001. It explains who the data processor will be for each of the interoperability measures proposed in this Regulation, sets out measures required from eu-LISA and Member State authorities to ensure the security of data processing, the confidentiality of data, the appropriate handling of security incidents and the appropriate monitoring of compliance with the measures in this Regulation. The chapter also contains provisions regarding the rights of data subjects, including the right to be informed that data regarding them has been stored and processed under this Regulation, and the right to access, correct and erase personal data that has been stored and processed under this Regulation. This chapter further sets out the principle that data processed under this Regulation must not be transferred or made available to any third country, international organisation or private party, with the exception of Interpol for some specific purposes, and data received from Europol via the European search portal where the rules of Regulation 2016/794 on subsequent data processing apply. Lastly, the chapter sets out the provisions relating to supervision and audit in relation to data protection.

Chapter VIII sets out the responsibilities eu-LISA before and after the entry into operations of the measures in this proposal, and for Member States, Europol and the ETIAS central unit.

Chapter IX sets out details relating to: statistical and reporting requirements relating to data processed under this Regulation; transitional measures that will be required; arrangements relating to costs arising from this Regulation; requirements relating to notifications; the process for the start of operations of measures proposed in this Regulation; governance arrangements including the formation of a committee and an advisory group, eu-LISA's responsibility in relation to training, and a practical handbook to support implementation and management of the interoperability components; procedures relating to monitoring and evaluation of the measures proposed in this Regulation; and provision for the entry into force of this Regulation.

2017/0352 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)

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 16(2), Article 74, Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2) thereof,

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor,

Having regard to the opinion of the European Economic and Social Committee,[43]

Having regard to the opinion of the Committee of the Regions,[44]

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In its Communication of 6 April 2016 entitled *Stronger and Smarter Information Systems for Borders and Security*[45], the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.

(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016[46], the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.

(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017[47], the European Parliament called for proposals to improve and develop existing EU information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.

---

[43] OJ C , , p. .

[44]

[45] COM(2016)205, 6.4.2016.

[46] Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

[47] European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP).

(4) The European Council of 15 December 2016[48] called for continued delivery on the interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017[49], the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements.

(6) In its Communication of 16 May 2017 entitled *Seventh progress report towards an effective and genuine Security Union*[50], the Commission set out, in line with its Communication of 6 April 2016 and confirmed by the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.

(7) In its Conclusions of 9 June 2017[51] on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability as proposed by the high-level expert group.

(8) The European Council of 23 June 2017[52] underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.

(9) With a view to improve the management of the external borders, to contribute to preventing and combating irregular migration and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, interoperability between EU information systems, namely the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and the [European Criminal Records Information System for third-country nationals (ECRIS-TCN)] should be established in order for these EU information systems and their data to supplement each other. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) The interoperability between the EU information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, contribute to fighting identity fraud, improve and harmonise data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the law enforcement access to the

---

48 http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/.
49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
50 COM(2017) 261 final, 16.5.2017.
51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.
52 European Council conclusions, 22-23 June 2017.

EES, the VIS, the [ETIAS] and Eurodac, and support the purposes of the EES, the VIS, the [ETIAS], Eurodac, the SIS and the [ECRIS-TCN system].

(11) The interoperability components should cover the EES, the VIS, the [ETIAS], Eurodac, the SIS, and the [ECRIS-TCN system]. They should also cover the Europol data to the extent of enabling it to be queried simultaneously with these EU information systems.

(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely third-country nationals whose personal data is processed in the EU information systems and by Europol, and to EU citizens whose personal data is processed in the SIS and by Europol.

(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and EU bodies to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the [ETIAS], Eurodac, the SIS, the [ECRIS-TCN system] and the Europol data. Enabling the simultaneous querying of all relevant EU information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or 'message broker' to search various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying systems.

(14) Those European search portal (ESP) end-users that have the right to access Europol data under Regulation (EU) 2016/794 of the European Parliament and of the Council[53] should be able to query the Europol data simultaneously with the EU information systems to which they have access. Any further data processing following such a query should take place in accordance with Regulation (EU) 2016/794, including restrictions on access or use imposed by the data provider.

(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.

(16) To ensure fast and systematic use of all EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system]. However, the national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union bodies to query the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol systems, complementing the existing dedicated interfaces.

(17) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. The shared biometric matching service (shared BMS) should be a technical tool to reinforce and facilitate

[53] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. The shared BMS should contribute to security, as well as financial, maintenance and operational benefits by relying on one unique technological component instead of different ones in each of the underlying systems. All automated fingerprint identification systems, including those currently used for Eurodac, the VIS and the SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates in one single location, facilitating cross-system comparisons using biometric data and enabling economies of scale in developing and maintaining the EU central systems.

(18) Biometric data constitute sensitive personal data. This regulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.

(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council[54], Regulation (EC) No 767/2008 of the European Parliament and of the Council[55], [the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat irregular migration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of the third-country nationals whose personal data are stored therein.

(20) The common identity repository (CIR) should therefore facilitate and assist in the correct identification of persons registered in the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system].

(21) Personal data stored in these EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for third-country nationals. The interoperability between EU information systems should contribute to the correct identification of third-country nationals. The common identity repository (CIR) should store the personal data concerning third-country nationals present in the systems that are necessary to enable the more accurate identification of those individuals, therefore including their identity, travel document and biometric data, regardless of the system in which the data was originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the

[54]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 (EES Regulation) (OJ L 327, 9.12.2017, p. 20–82).

[55] 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).

underlying systems and should be automatically deleted when the data is deleted in the underlying systems in accordance with their logical separation.

(22) The new processing operation consisting in the storage of such data in the common identity repository (CIR) instead of the storage in each of the separate systems is necessary to increase the accuracy of the identification that is made possible by the automated comparison and matching of such data. The fact that the identity and biometric data of third-country nationals is stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system Regulations, as the CIR should be a new shared component of those underlying systems.

(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, is necessary to achieve the purpose of correct identification of third-country nationals within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.

(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to facilitate and streamline access by law enforcement authorities to the EU information systems that are not established exclusively for purposes of prevention, investigation, detection or prosecution of serious crime.

(25) The common identity repository (CIR) should provide for a shared container for identity and biometric data of third-country nationals registered in the EES, the VIS, [the ETIAS], Eurodac and the [ECRIS-TCN system], serving as the shared component between these systems for storage of this data, and to allow its querying.

(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.

(27) In order to ensure the correct identification of a person, Member State authorities competent for preventing and combating irregular migration and competent authorities within the meaning of Article 3(7) of Directive 2016/680 should be allowed to query the common identity repository (CIR) with the biometric data of that person taken during an identity check.

(28) Where the biometric data of the person cannot be used or if the query with that data fails, the query should be carried out with identity data of that person in combination with travel document data. Where the query indicates that data on that person are stored in the common identity repository (CIR), Member State authorities should have access to consult the identity data of that person stored in the CIR, without providing any indication as to which EU information system the data belongs to.

(29) Member States should adopt national legislative measures designating the authorities competent to perform identity checks with the use of the common identity repository (CIR) and laying down the procedures, conditions and criteria of such checks in line with the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before the member of those authorities should be provided for by national legislative measures.

(30) This Regulation should also introduces a new possibility for streamlined access to data beyond identity data present in the EES, the VIS, [the ETIAS] or Eurodac by Member State designated law enforcement authorities and Europol. Data, including data other than identity data contained in those systems, may be necessary for the prevention, detection, investigation and prosecution of terrorist offences or serious criminal offences in a specific case.

(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, beyond the relevant identity data covered under common identity repository (CIR) obtained using biometric data of that person taken during an identity check, should continue to be governed by the provisions in the respective legal instruments. The designated law enforcement authorities and Europol do not know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a hit in the system (a so-called hit-flag functionality).

(32) The logs of the queries of the common identity repository should indicate the purpose of the query. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, therefore indicating that such query was launched for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences.

(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a hit-flag type of response indicating the data is recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A hit-flag would not reveal personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems. No adverse decision for the concerned individual should be made by the authorised end-user solely on the basis of the simple occurrence of a hit-flag. Access by the end-user of a hit-flag would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated authority and Europol to address its request for access for personal data more effectively directly to the system that was flagged as containing it.

(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) should enable identifying the information system that knows the person in one single search. By creating the obligation to use this new law enforcement access approach in these cases, access to the personal data stored in the EES, the VIS, [the ETIAS] and Eurodac should take place without the requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA. The principle of prior search effectively limits the possibility of Member State' authorities to consult systems for justified law enforcement purposes and could thereby result in missed opportunities to uncover necessary information. The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification

system of other Member States under Decision 2008/615/JHA should only cease to apply once the alternative safeguard of the two-step approach to law enforcement access through the CIR has become operational.

(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system]. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored therein.

(36) The possibility to achieve the objectives of the EU information systems is undermined by the current inability for the authorities using these systems to conduct sufficiently reliable verifications of the identities of the third-country nationals whose data are stored in different systems. That inability is determined by the fact that the set of identity data stored in a given individual system may be fraudulent, incorrect, or incomplete, and that there is currently no possibility to detect such fraudulent, incorrect or incomplete identity data by way of comparison with data stored in another system. To remedy this situation it is necessary to have a technical instrument at Union level allowing accurate identification of third-country nationals for these purposes.

(37) The multiple-identity detector (MID) should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The MID should only contain the links between individuals present in more than one EU information system, strictly limited to the data necessary to verify that a person is recorded lawfully or unlawfully under different biographical identities in different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems should be kept to an absolute minimum and therefore is limited to a multiple-identity detection at the time new data is added to one of the information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.

(38) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly. This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union, the effective implementation of the Union's asylum and visa policies and the fight against irregular migration.

(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created by a national authority or an EU body. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the third-country national stored across

several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and the SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the concerned third-country national.

(40) The national authority or EU body that recorded the data in the respective EU information system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.

(41) Access to the multiple-identity detector (MID) by Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person, or where the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person. Where the linked identity data is not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.

(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a hit resulting in a link with data already stored in another EU information system. The authority responsible for the verification of multiple identities should assess whether there are multiple lawful or unlawful identities. Such assessment should be performed where possible in the presence of the third-country national and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law.

(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure, on persons for discreet checks or specific checks or on unknown wanted persons, the authority responsible for the verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with the [SIS Regulations].

(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible to develop a central monitoring capacity for data quality and to produce regular data analysis reports to improve the control of implementation and application by Member States of EU information systems. The common quality indicators should include the minimum quality standards to store data in the EU information systems or the interoperability components. The goal of such a data quality standards should be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.

(45) The Commission should evaluate eu-LISA quality reports and should issue recommendations to Member States where appropriate. Member States should be

responsible for preparing an action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.

(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate interoperability by enabling the creation and reading of the contents of the exchange in a consistent and semantically equivalent manner.

(47) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes. eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository, the multiple-identity detector and the shared biometric matching service (shared BMS). The data contained in the CRRS should not enable the identification of individuals. eu-LISA should render the data anonymous and should record such anonymous data in the CRRS. The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU information systems or in the interoperability components.

(48) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, when Directive (EU) 2016/680 of the European Parliament and of the Council should apply.

(49) The specific provisions on data protection of [the Eurodac Regulation], [the Regulation on SIS in the field of law enforcement], [the Regulation on SIS in the field of illegal return] and [the ECRIS-TCN System Regulation] should apply to the processing of personal data in those respective systems.

(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council[56] should apply to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794, which should apply to the processing of personal data by Europol.

(51) The national supervisory authorities established in accordance with [Regulation (EU) 2016/679] should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data by interoperability components.

(52) "(...) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on … "

[56] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.

(54) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues. eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity regarding the development, design and management of the interoperability components.

(55) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, institutions and bodies identified in this Regulation to consult certain data related to certain interoperability components without enabling individual identification.

(56) In order to allow competent authorities and the EU bodies to adapt to the new requirements on the use of the European search portal (ESP), it is necessary to provide for a transitional period. Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID), transitional measures should be established for the start of its operations.

(57) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[57]. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.

(58) In order to supplement certain detailed technical aspects of this Regulation, 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 the profiles for the users of the European search portal (ESP) and the content and format of the ESP replies. 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[58]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(59) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: automated data quality control mechanisms, procedures and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; the operation of the central repository for reporting and statistics; and cooperation procedure in case of security incidents. Those powers should be exercised

[57] Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

[58] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[59].

(60) Regulation 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.

(61) This Regulation is without prejudice to the application of Directive 2004/38/EC.

(62) In accordance with Article 3 of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention[60], Denmark is to notify the Commission whether it will implement the contents of this Regulation, insofar as it relates to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)].

(63) Insofar as its provisions relate to SIS as governed by Decision 2007/533/JHA, the United Kingdom is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the Schengen *acquis*) and Article 8(2) of Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*[61]. Furthermore, insofar as its provisions relate to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)] the United Kingdom may notify to the President of the Council its wish to take part in the adoption and application of this Regulation, in accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU (Protocol on the position of the United Kingdom and Ireland). Insofar as its provisions relate to [the ECRIS-TCN system], in accordance with Articles 1 and 2 and Article 4a(1) of Protocol 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and the TFEU, the United Kingdom is not taking part in the adoption of this Regulation and is not bound or subject to its application. In accordance with Article 3 and Article 4a(1) of Protocol 21, the United Kingdom may notify its wish to take part in the adoption of this Regulation.

(64) Insofar as its provisions relate to SIS as governed by Decision 2007/533/JHA, Ireland is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on

---

59 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 the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

60

61

the Schengen *acquis* integrated into the framework of the European Union, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the Schengen *acquis*), and 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*[62]. Furthermore, insofar as its provisions relate to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)], Ireland may notify to the President of the Council its wish to take part in the adoption and application of this Regulation, in accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the position of the United Kingdom and Ireland). Insofar as its provisions relate to [the ECRIS-TCN system], in accordance with Articles 1 and 2 and Article 4a(1) of Protocol 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and the TFEU, Ireland is not taking part in the adoption of this Regulation and is not bound or subject to its application. In accordance with Article 3 and Article 4a(1) of Protocol 21, Ireland may notify its wish to take part in the adoption of this Regulation.

(65) As regards Iceland and Norway, as regards Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)], this Regulation constitutes a new measure within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway.

(66) As regards Switzerland, as regards Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)], this Regulation constitutes a new measure related to Eurodac within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland.

(67) As regards Liechtenstein, as regards Eurodac, [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX establishing the criteria and mechanisms for determining the Member State

62

responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)] this Regulation constitutes a new measure within the meaning of the Protocol between 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 Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland.

(68) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles,

HAVE ADOPTED THIS REGULATION:

CHAPTER I
General provisions

Article 1
Subject matter

1. This Regulation, together with [Regulation 2018/xx on interoperability borders and visa], establishes a framework to ensure the interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)] in order for those systems and data to supplement each other.

2. The framework shall include the following interoperability components:

   (a) a European search portal (ESP);

   (b) a shared biometric matching service (shared BMS);

   (c) a common identity repository (CIR);

   (d) a multiple-identity detector (MID).

3. This Regulation also lays down provisions on data quality requirements, on a Universal Message Format (UMF), on a central repository for reporting and statistics (CRRS) and lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design and operation of the interoperability components.

4. This Regulation also adapts the procedures and conditions for Member State law enforcement authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) access to the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS),] and Eurodac for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.

Article 2
Objectives of interoperability

1. By ensuring interoperability, this Regulation shall have the following objectives:
   (a) to improve the management of the external borders;
   (b) to contribute to preventing and combating irregular migration;
   (c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;
   (d) to improve the implementation of the common visa policy; and
   (e) to assist in examining application for international protection.
2. The objectives of ensuring interoperability shall be achieved by:
   (a) ensuring the correct identification of persons;
   (b) contributing to fighting identity fraud;
   (c) improving and harmonising data quality requirements of the respective EU information systems;
   (d) facilitating the technical and operational implementation by Member States of existing and future EU information systems;
   (e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems;
   (f) streamlining the conditions for law enforcement access to the EES, the VIS, [the ETIAS] and Eurodac;
   (g) supporting the purposes of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].

Article 3
Scope

1. This Regulation applies to Eurodac, the Schengen Information System (SIS) and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)].
2. This Regulation also applies to the Europol data to the extent of enabling querying it simultaneously to the EU information systems referred to in paragraph 1 in accordance with Union law.
3. This Regulation applies to persons in respect of whom personal data may be processed in the EU information systems referred to in paragraph 1 and in the Europol data referred to in paragraph 2.

Article 4
Definitions

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

(1) ‘external borders’ means external borders as defined in Article 2(2) of Regulation (EU) 2016/399;

(2) ‘border checks’ means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;

(3) ‘border authority’ means the border guard assigned in accordance with national law to carry out border checks;

(4) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;

(5) ‘verification’ means the process of comparing sets of data to establish the validity of a claimed identity (one-to-one check);

(6) ‘identification’ means the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check);

(7) ‘third-country national’ means a person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown;

(8) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;

(9) ‘identity data’ means the data referred to in Article 27(3)(a) to (h);

(10) ‘fingerprint data’ means the data relating to the fingerprints of an individual;

(11) ‘facial image’ means digital images of the face;

(12) ‘biometric data’ means fingerprint data and/or facial image;

(13) ‘biometric template’ means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications;

(14) ‘travel document’ means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed;

(15) ‘travel document data’ means the type, number and country of issuance of the travel document, the date of expiry of the validity of the travel document and the three-letter code of the country issuing the travel document;

(16) ‘travel authorisation’ means travel authorisation as defined in Article 3 of the [ETIAS Regulation];

(17) ‘short-stay visa’ means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009;

(18) ‘EU information systems’ means the large-scale IT systems managed by eu-LISA;

(19) ‘Europol data’ means personal data provided to Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794;

(20) ‘Interpol databases’ means the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN);

(21) ‘match’ means the existence of a correspondence established by comparing two or more occurrences of personal data recorded or being recorded in an information system or database;

(22) ‘hit’ means the confirmation of one match or several matches;

(23) 'police authority' means 'competent authority' as defined in Article 3(7) of Directive 2016/680;

(24) ‘designated authorities’ means the Member State designated authorities referred to in Article 29(1) of Regulation (EU) 2017/2226, Article 3(1) of Council Decision 2008/633/JHA, [Article 43 of the ETIAS Regulation] and [Article 6 of the Eurodac Regulation];

(25) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;

(26) ‘serious criminal offence’ means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;

(27) 'EES' means the Entry/Exit System as referred to in Regulation (EU) 2017/2226;

(28) 'VIS' means the Visa Information System as referred to in Regulation (EC) No 767/2008;

(29) ['ETIAS' means the European Travel Information and Authorisation System as referred to in the ETIAS Regulation];

(30) 'Eurodac' means Eurodac as referred to in the [Eurodac Regulation];

(31) 'SIS' means the Schengen Information System as referred to [in the Regulation on SIS in the field of border checks, Regulation on SIS in the field of law enforcement and Regulation on SIS in the field of illegal return];

(32) ['ECRIS-TCN System' means the European Criminal Records Information System holding conviction information on third-country national and stateless persons as referred to in the ECRIS-TCN System Regulation];

(33) 'ESP' means the European search portal as referred to in Article 6;

(34) 'shared BMS' means the shared biometric matching service as referred to in Article 15;

(35) 'CIR' means the common identity repository as referred to in Article 17;

(36) 'MID' means the multiple-identity detector as referred to in Article 25;

(37) 'CRRS' means the central repository for reporting and statistics as referred to in Article 39.

Article 5
Non-discrimination

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. Particular attention shall be paid to children, the elderly and persons with a disability.

CHAPTER II
European Search Portal

Article 6
European search portal

1. A European search portal (ESP) is established for the purposes of ensuring that Member State authorities and EU bodies have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases that they need to perform their tasks in accordance with their access rights and of supporting the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] and the Europol data.

2. The ESP shall be composed of:

   (a) a central infrastructure, including a search portal enabling the simultaneous querying of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] as well as of the Europol data and the Interpol databases;

   (b) a secure communication channel between the ESP, Member States and EU bodies that are entitled to use the ESP in accordance with Union law;

   (c) a secure communication infrastructure between the ESP and the EES, the VIS, [the ETIAS], Eurodac, the Central-SIS, [the ECRIS-TCN system], the Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the common identity repository (CIR) and the multiple-identity detector.

3. eu-LISA shall develop the ESP and ensure its technical management.

Article 7
Use of the European search portal

1. The use of the ESP shall be reserved to the Member State authorities and EU bodies having access to the EES, [the ETIAS], the VIS, the SIS, Eurodac and [the ECRIS-TCN system], to the CIR and the multiple-identity detector as well as the Europol data and the Interpol databases in accordance with Union or national law governing such access.

2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of Eurodac and [the ECRIS-TCN system] in accordance with their access rights under Union and national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.

3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in the [Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement]. Access to the Central SIS via the ESP shall be established through the national system (N.SIS) of each Member State in accordance with [Article 4(2) of the Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement].

4. The EU bodies shall use the ESP to search data related to persons or their travel documents in the Central SIS.

5. The authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Europol data in accordance with their access rights under Union and national law.

Article 8
Profiles for the users of the European search portal

1. For the purposes of enabling the use of the ESP, eu-LISA shall create a profile for each category of user of the ESP in accordance with the technical details and access rights referred to in paragraph 2, including, in accordance with Union and national law:

   (a) the fields of data to be used for querying;

   (b) the EU information systems, the Europol data and the Interpol databases that shall and may be consulted and that shall provide a reply to the user; and

   (c) the data provided in each reply.

2. The Commission shall adopt delegated acts in accordance with Article 63 to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights.

Article 9
Queries

1. The users of the ESP shall launch a query by introducing data in the ESP in accordance with their user profile and access rights. Where a query has been launched, the ESP shall query simultaneously, with the data introduced by the user of the ESP, the EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system] and the CIR as well as the Europol data and the Interpol databases.

2. The fields of data used to launch a query via the ESP shall correspond to the fields of data related to persons or travel documents that may be used to query the various EU information systems, the Europol data and the Interpol databases in accordance with the legal instruments governing them.

3. eu-LISA shall implement an interface control document (ICD) based on the UMF referred to in Article 38 for the ESP.

4. The EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system], the CIR and the multiple-identity detector, as well as the Europol data and the Interpol databases, shall provide the data that they contain resulting from the query of the ESP.

5. When querying the Interpol databases, the design of the ESP shall ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data.

6. The reply to the user of the ESP shall be unique and shall contain all the data to which the user has access under Union law. Where necessary, the reply provided by the ESP shall indicate to which information system or database the data belongs.

7. The Commission shall adopt a delegated act in accordance with Article 63 to specify the content and format of the ESP replies.

Article 10
Keeping of logs

1. Without prejudice to [Article 39 of the Eurodac Regulation], [Articles 12 and 18 of the Regulation on SIS in the field of law enforcement], [Article 29 of the ECRIS-TCN Regulation] and Article 40 of Regulation (EU) 2016/794, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:

   (a) the Member State authority and the individual user of the ESP, including the ESP profile used as referred to in Article 8;

   (b) the date and time of the query;

   (c) the EU information systems and the Europol data queried;

   (d) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.

2. The logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun.

Article 11
Fall-back procedures in case of technical impossibility to use the European search portal

1. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP shall be notified by eu-LISA.

2. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the national infrastructure in a Member State, that Member State's competent authority shall notify eu-LISA and the Commission.

3. In both scenarios, and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States may access the information systems referred to in Article 9(1) or the CIR directly using their respective national uniform interfaces or national communication infrastructures.

CHAPTER III
Shared Biometric Matching Service

Article 12
Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates and enabling querying with biometric data across several EU information systems is

established for the purposes of supporting the CIR and the multiple-identity detector and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].

2. The shared BMS shall be composed of:

   (a) a central infrastructure, including a search engine and the storage of the data referred to in Article 13;

   (b) a secure communication infrastructure between the shared BMS, Central-SIS and the CIR.

3. eu-LISA shall develop the shared BMS and ensure its technical management.

Article 13
Data stored in the shared biometric matching service

1. The shared BMS shall store the biometric templates that it shall obtain from the following biometric data:

   (a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) of Regulation (EU) 2017/2226;

   (b) the data referred to in Article 9(6) of Regulation (EC) No 767/2008;

   (c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks;

   (d) the data referred to in Article 20(3)(w) and (x) of the Regulation on SIS in the field of law enforcement;

   (e) the data referred to in Article 4(3)(t) and (u) of the Regulation on SIS in the field of illegal return];

   (f) [the data referred to in Article 13(a) of the Eurodac Regulation;]

   (g) [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation.]

2. The shared BMS shall include in each biometric template a reference to the information systems in which the corresponding biometric data is stored.

3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard.

4. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).

Article 14
Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in the EES Regulation, the VIS Regulation, the Eurodac Regulation, the [SIS Regulations] and [the ECRIS-TCN Regulation].

Article 15
Data retention in the shared biometric matching service

The data referred to in Article 13 shall be stored in the shared BMS for as long as the corresponding biometric data is stored in the CIR or the SIS.

Article 16
Keeping of logs

1. Without prejudice to [Article 39 of the Eurodac Regulation], [Article 12 and 18 of the Regulation on SIS in the field of law enforcement] and [Article 29 of the ECRIS-TCN Regulation], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include, in particular, the following:

   (a) the history related to the creation and storage of biometric templates;

   (b) a reference to the EU information systems queried with the biometric templates stored in the shared BMS;

   (c) the date and time of the query;

   (d) the type of biometric data used to launch the query;

   (e) the length of the query;

   (f) the results of the query and date and time of the result;

   (g) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.

2. The logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun. The logs referred to in paragraph 1(a) shall be erased once the data is erased.

CHAPTER IV
Common Identity Repository

Article 17
Common identity repository

1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system], of supporting the functioning of the multiple-identity detector and of facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime.

2. The CIR shall be composed of:

(a) a central infrastructure that shall replace the central systems of respectively the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system] to the extent that it shall store the data referred to in Article 18;

(b) a secure communication channel between the CIR, Member States and EU bodies that are entitled to use the European search portal (ESP) in accordance with Union law;

(c) a secure communication infrastructure between the CIR and the EES, [the ETIAS], the VIS, Eurodac and [the ECRIS-TCN system] as well as with the central infrastructures of the ESP, the shared BMS and the multiple-identity detector.

3. eu-LISA shall develop the CIR and ensure its technical management.

Article 18
The common identity repository data

1. The CIR shall store the following data – logically separated – according to the information system from which the data was originated:

(a) – (not applicable);

(b) – (not applicable);

(c) – (not applicable);

(d) [the data referred to in Article 13(a) to (e), (g) and (h) of the [Eurodac Regulation;]

(e) [the data referred to in Article 5(1)(b) and 5(2) and the following data of Article 5(1)(a) of the ECRIS-TCN Regulation: surname or family name; first name(s) (given name(s)); sex; date of birth; place and country of birth; nationality or nationalities; gender and where applicable previous names, pseudonyms(s) and/or alias name(s).]

2. For each set of data referred to in paragraph 1, the CIR shall include a reference to the information systems to which the data belongs.

3. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).

Article 19
Adding, amending and deleting data in the common identity repository

1. Where data is added, amended or deleted in Eurodac or [the ECRIS-TCN system], the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.

2. Where the multiple-identity detector creates a white or red link in accordance with Articles 32 and 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.

Article 20

Access to the common identity repository for identification

1. Where a Member State police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.

   Where the query indicates that data on that person is stored in the CIR, the Member States authority shall have access to consult the data referred to in Article 18(1).

   Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel document data, or with the identity data provided by that person.

2. Member States wishing to avail themselves of the possibility provided for in this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks within the purposes referred to in Article 2(1)(b) and (c). They shall designate the police authorities competent and lay down the procedures, conditions and criteria of such checks.

Article 21

Access to the common identity repository for the detection of multiple identities

1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the verification of different identities determined in accordance with Article 29 shall have access, solely for the purpose of that verification, to the identity data stored in the CIR belonging to the various information systems connected to a yellow link.

2. Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of fighting identity fraud, to the identity data stored in the CIR belonging to the various information systems connected to a red link.

Article 22

Querying the common identity repository for law enforcement purposes

1. For the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case and in order to obtain information on whether data on a specific person is present in Eurodac, the Member State designated authorities and Europol may consult the CIR.

2. Member State designated authorities and Europol shall not be entitled to consult data belonging to [the ECRIS-TCN] when consulting the CIR for the purposes listed in paragraph 1.

3. Where, in reply to a query the CIR indicates data on that person is present in Eurodac the CIR shall provide to Member States' designated authorities and Europol a reply in the form of a reference indicating which of the information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised.

4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legislative instruments governing such access.

Article 23
Data retention in the common identity repository

1. The data referred to in Article 18(1) and (2) shall be deleted from the CIR in accordance with the data retention provisions of [the Eurodac Regulation] and [the ECRIS-TCN Regulation] respectively.

2. The individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the information systems whose data is contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data.

Article 24
Keeping of logs

1. Without prejudice to [Article 39 of the Eurodac Regulation] and [Article 29 of the ECRIS-TCN Regulation], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.

2. Concerning any access to the CIR pursuant to Article 20, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:

   (a) the purpose of access of the user querying via the CIR;

   (b) the date and time of the query;

   (c) the type of data used to launch the query;

   (d) the results of the query;

   (e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.

3. Concerning any access to the CIR pursuant to Article 21, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:

   (a) the purpose of access of the user querying via the CIR;

   (b) the date and time of the query;

   (c) where relevant, the data used to launch the query;

   (d) where relevant, the results of the query;

   (e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.

4. Concerning any access to the CIR pursuant to Article 22, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:

(a) the national file reference;

(b) the date and time of the query;

(c) the type of data used to launch the query;

(d) the results of the query;

(e) the name of the authority consulting the CIR;

(f) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the official who carried out the query and of the official who ordered the query.

The logs of such access shall be regularly verified by the competent supervisory authority established in accordance with Article 51 of Regulation (EU) 2016/679 or in accordance with Article 41 of Directive 2016/680, at intervals not exceeding six months, to verify whether the procedures and conditions set out in Article 22(1) to (3) are fulfilled.

5. Each Member State shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Articles 20, 21 and 22.

6. The logs referred to in paragraphs 1 and 5 may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. They shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun.

7. eu-LISA shall keep the logs related to the history of the data stored in individual file, for purposes defined in paragraph 6. The logs related to the history of the data stored shall be erased once the data is erased.

CHAPTER V
Multiple-identity Detector

Article 25
Multiple-identity detector

1. A multiple-identity detector (MID) creating and storing links between data in the EU information systems included in the common identity repository (CIR) and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].

2. The MID shall be composed of:

(a) a central infrastructure, storing links and references to information systems;

(b) a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the European search portal and the CIR.

3. eu-LISA shall develop the MID and ensure its technical management.

Article 26
Access to the multiple-identity detector

1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

   (a) – (not applicable);

   (b) – (not applicable);

   (c) – (not applicable);

   (d) the authorities competent to assess a request for international protection provided for in the Eurodac Regulation when assessing a new request for international protection;

   (e) the SIRENE Bureaux of the Member State creating a [Regulation on SIS in the field of law enforcement or Regulation on SIS in the field of illegal return];

   (f) [the central authorities of the convicting Member State when recording or updating data in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

2. Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.

Article 27
Multiple-identity detection

1. A multiple-identity detection in the common identity repository and the SIS shall be launched where:

   (a) – (not applicable);

   (b) – (not applicable);

   (c) – (not applicable);

   (d) [an application for international protection is created or updated in Eurodac in accordance with Article 10 of the Eurodac Regulation];

   (e) [an alert on a person is created or updated in the SIS in accordance with Chapters VI, VII, VIII and IX of the Regulation on SIS in the field of law enforcement and Article 3 of the Regulation on SIS in the field of illegal return];

   (f) [a data record is created or updated in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

2. Where the data contained within an information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central-SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national is already stored in the CIR or in the Central SIS.

3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in the CIR and the Central-SIS using the following data:

(a) – (not applicable);

(b) – (not applicable);

(c) – (not applicable);

(d) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 12 of the Eurodac Regulation];

(e) – (not applicable);

(f) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(3) of the Regulation on SIS in the field of law enforcement;]

(g) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 4 of the Regulation on SIS in the field of illegal return;]

(h) [surname (family name); first name(s) (given names); date of birth, place of birth, nationality(ies) and gender as referred to in Article 5(1)(a) of the ECRIS-TCN Regulation.]

4. The multiple-identity detection shall only be launched in order to compare data available in one information system with data available in other information systems.

Article 28
Results of the multiple-identity detection

1. Where the queries referred to in Article 27(2) and (3) do not report any hit, the procedures referred to in Article 27(1) shall continue in accordance with the respective Regulations governing them.

2. Where the query laid down in Article 27(2) and (3) reports one or several hit(s), the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the hit.

Where several hits are reported, a link shall be created between all data triggering the hit. Where data was already linked, the existing link shall be extended to the data used to launch the query.

3. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

4. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.

5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as identical or similar in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

6. The links shall be stored in the identity confirmation file referred to in Article 34.

The Commission shall lay down the technical rules for linking data from different information systems by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 29
Manual verification of different identities

1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:

(a) – (not applicable);

(b) – (not applicable);

(c) – (not applicable);

(d) the authority assessing a request for international protection as provided for in the Eurodac Regulation for hits that occurred when assessing such request;

(e) the SIRENE Bureaux of the Member State for hits that occurred when creating a SIS alert in accordance with the [Regulations on SIS in the field of law enforcement and on SIS in the field of illegal return];

(f) the central authorities of the convicting Member State for hits that occurred when recording or updating data in the ECRIS-TCN system in accordance with Article 5 of the [ECRIS-TCN Regulation].

The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification file.

2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:

(a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement];

(b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement];

(c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement];

(d) [in an alert on return in accordance with the Regulation on SIS in the field of illegal return];

(e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement];

(f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].

3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant

identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS, and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file without delay.

4. – (not applicable).

5. Where more than one link is obtained, the authority responsible for the verification of different identities shall assess each link separately.

6. Where data reporting a hit was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.

Article 30
Yellow link

1. A link between data from two or more information systems shall be classified as yellow in any of the following cases:

   (a) the linked data shares the same biometric but different identity data and no manual verification of different identity has taken place;

   (b) the linked data has different identity data and no manual verification of different identity has taken place.

2. Where a link is classified as yellow in accordance with paragraph 1, the procedure laid down in Article 29 applies.

Article 31
Green link

1. A link between data from two or more information systems shall be classified as green where the linked data do not share the same biometric but have similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.

2. Where the common identity repository (CIR) or the SIS are queried and where a green link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data does not correspond to the same person. The queried information system shall reply indicating only the data of the person whose data was used for the query, without triggering a hit against the data that is subject to the green link.

Article 32
Red link

1. A link between data from two or more information systems shall be classified as red in any of the following cases:

   (a) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person;

   (b) the linked data has similar identity data and the authority responsible for the

verification of different identities concluded it refers unlawfully to the same person.

2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law.

3. Where a red link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN System], the individual file stored in the CIR shall be updated in accordance with Article 19(1).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities.

5. Where a red link is created, the authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.

Article 33
White link

1. A link between data from two or more information systems shall be classified as white in any of the following cases:

   (a) the linked data shares the same biometric and the same or similar identity data;

   (b) the linked data shares the same or similar identity data and at least one of the information systems does not have biometric data on the person;

   (c) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers to the same person legally having different identity data.

2. Where the CIR or the SIS are queried and where a white link exists between one or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data correspond to the same person. The queried information systems shall reply indicating, where relevant, all the linked data on the person, hence triggering a hit against the data that is subject to the white link, if the authority launching the query has access to the linked data under Union or national law.

3. Where a white link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system], the individual file stored in the CIR shall be updated in accordance with Article 19(1).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], where a white link is created following a manual verification of multiple identities, the authority responsible for verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.

Article 34
Identity confirmation file

The identity confirmation file shall contain the following data:

(a) the links, including their description in form of colours, as referred to in Articles 30 to 33;

(b) a reference to the information systems whose data is linked;

(c) a single identification number allowing to retrieve the data from the information systems of corresponding linked files;

(d) where relevant, the authority responsible for the verification of different identities.

Article 35
Data retention in the multiple-identity detector

The identity confirmation files and its data, including the links, shall be stored in the multiple-identity detector (MID) only for as long as the linked data is stored in two or more EU information systems.

Article 36
Keeping of logs

1. eu-LISA shall keep logs of all data processing operations within the MID. Those logs shall include, in particular, the following:

   (a) the purpose of access of the user and his or her access rights;

   (b) the date and time of the query;

   (c) the type of data used to launch the query or queries;

   (d) the reference to the data linked;

   (e) the history of the identity confirmation file;

   (f) the identifying mark of the person who carried out the query.

2. Each Member State shall keep logs of the staff duly authorised to use the MID.

3. The logs may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. The logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun. The logs related to the history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased.

CHAPTER VI
Measures supporting interoperability

Article 37
Data quality

1. eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the SIS, Eurodac, [the ECRIS-TCN system], the shared biometric matching service (shared BMS), the common identity repository (CIR) and the multiple-identity detector (MID).

2. eu-LISA shall establish common data quality indicators and the minimum quality standards to store data in the SIS, Eurodac, [the ECRIS-TCN system], the shared BMS, the CIR and the MID.

3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned.

4. The details of the automated data quality control mechanisms and procedures and the common data quality indicators and the minimum quality standards to store data in the SIS, Eurodac, [the ECRIS-TCN system], the shared BMS, the CIR and the MID, in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

5. One year after the establishment of the automated data quality control mechanisms and procedures and common data quality indicators and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall report on any progress against this action plan until it is fully implemented. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[63]

Article 38
Universal Message Format

1. The Universal Message Format (UMF) standard is hereby established. The UMF defines standards for certain content elements of cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs

2. The UMF standard shall be used in the development of the [Eurodac], the [ECRIS-TCN system], the European search portal, the CIR, the MID and, if appropriate, in the development by eu-LISA or any other EU body of new information exchange models and information systems in the area of Justice and Home Affairs.

[63] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

3. The implementation of the UMF standard may be considered in the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States or associated countries.

4. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 39
Central repository for reporting and statistics

1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of Eurodac, the SIS and [the ECRIS-TCN system] and to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

2. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in [Article 42(8) of the Eurodac Regulation], [Article 71 of the Regulation on SIS in the field of law enforcement] and [Article 30 of the ECRIS-TCN Regulation] logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the repository shall be granted by means of secured access through the Trans- European Services for Telematics between Administrations (TESTA) network service with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in [Article 42(8) of the Eurodac Regulation], [Article 71 of the Regulation on SIS in the field of law enforcement] and [Article 30 of the ECRIS-TCN Regulation].

3. eu-LISA shall render the data anonymous and shall record such anonymous data in the CRRS. The process for rendering the data anonymous shall be automated.

4. The CRRS shall be composed of:

   (a) a central infrastructure, consisting of a data repository enabling the rendering of anonymous data;

   (b) a secure communication infrastructure to connect the CRRS to the SIS, Eurodac and [the ECRIS-TCN], as well as the central infrastructures of the shared BMS, the CIR and the MID.

5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

CHAPTER VII
Data protection

Article 40
Data controller

1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the Eurodac, SIS and [the ECRIS-TCN system] respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS.

2. In relation to the processing of data in the common identity repository (CIR), the Member State authorities that are controllers for the Eurodac and [the ECRIS-TCN system] respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.

3. In relation to the processing of data in the multiple-identity detector:

   (a) the European Border and Coast Guard Agency shall be considered a data controller in accordance with Article 2(b) of Regulation No 45/2001 in relation to processing of personal data by the ETIAS Central Unit;

   (b) the Member State authorities adding or modifying the data in the identity confirmation file are also to be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of the personal data in the multiple-identity detector;

Article 41
Data processor

In relation to the processing of personal data in the CIR, eu-LISA is to be considered the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001.

Article 42
Security of processing

1. Both eu-LISA and the Member State authorities shall ensure the security of the processing of personal data that takes place pursuant to the application of this Regulation. eu-LISA, [the ETIAS Central Unit] and the Member State authorities shall cooperate on security-related tasks.

2. Without prejudice to Article 22 of Regulation (EC) No 45/2001, eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.

3. In particular, eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

   (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) prevent the unauthorised reading, copying, modification or removal of data media;

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

(d) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;

(e) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(f) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

(g) ensure that it is possible to verify and establish what data has been processed in the interoperability components, when, by whom and for what purpose;

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;

(i) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation.

4. Member States shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.

Article 43
Confidentiality of SIS data

1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.

Article 44
Security incidents

1. Any event that has or may have an impact on the security of the interoperability components and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed so as to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the Commission, eu-LISA and the European Data Protection Supervisor of security incidents. In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor.

4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States and reported in compliance with the incident management plan to be provided by eu-LISA.

5. The Member States concerned and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specification of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 45
Self-monitoring

Member States and the relevant EU bodies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.

The data controllers as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of logs, and cooperate, where necessary, with the supervisory authorities referred to in Articles 49 and 50.

Article 46
Right of information

1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared biometric matching service, the common identity repository or the multiple-identity detector shall be informed by the authority collecting their data, at the time their data are collected, about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, and about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.

2. Persons whose data is recorded in Eurodac or [the ECRIS-TCN system] shall be informed about the processing of data for the purposes of this Regulation in accordance with paragraph 1 when:

(a) – (not applicable);

(b) – (not applicable);

(c) – (not applicable);

(d) [an application for international protection is created or updated in Eurodac in accordance with Article 10 of the Eurodac Regulation];

(e) [a data record is created or updated in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

Article 47
Right of access, correction and erasure

1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679, any person shall have the right to address him or herself to the Member State responsible for the manual verification of different identities or of any Member State, who shall examine and reply to the request.

2. The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made shall reply to such requests within 45 days of receipt of the request.

3. If a request for correction or erasure of personal data is made to a Member State other than the Member State responsible, the Member State to which the request has been made shall contact the authorities of the Member State responsible within seven days and the Member State responsible shall check the accuracy of the data and the lawfulness of the data processing within 30 days of such contact.

4. Where, following an examination, it is found that the data stored in the multiple-identity detector (MID) are factually inaccurate or have been recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall correct or delete these data.

5. Where data in the MID is amended by the responsible Member State during its validity period, the responsible Member State shall carry out the processing laid down in Article 27 and, where relevant, Article 29 to determine whether the amended data shall be linked. Where the processing does not report any hit, the responsible Member State or, where applicable, the Member State to which the request has been made shall delete the data from the identity confirmation file. Where the automated processing reports one or several hit(s), the responsible Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

6. Where the responsible Member State or, where applicable, the Member State to which the request has been made does not agree that data stored in the MID are factually inaccurate or have been recorded unlawfully, that Member State shall adopt an administrative decision explaining in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him or her.

7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred in paragraph 3 and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the competent national supervisory authorities.

8. Any request made pursuant to paragraph 3 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 3 and shall be erased immediately afterwards.

9. The responsible Member State or, where applicable, the Member State to which the request has been made shall keep a record in the form of a written document that a request referred to in paragraph 3 was made and how it was addressed, and shall make that document available to competent data protection national supervisory authorities without delay.

Article 48
Communication of personal data to third countries, international organisations and private parties

Personal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party.

Article 49
Supervision by the national supervisory authority

1. The supervisory authority or authorities designated pursuant to Article 49 of Regulation (EU) 2016/679 shall ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every four years.

2. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

Article 50
Supervision by the European Data Protection Supervisor

The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the Member States. eu-LISA shall be given an opportunity to make comments before the reports are adopted.

Article 51
Cooperation between national supervisory authorities and the European Data Protection Supervisor

1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) XXXX/2018 [revised Regulation 45/2001].

CHAPTER VIII
Responsibilities

Article 52
Responsibilities of eu-LISA during the design and development phase

1. eu-LISA shall ensure that the central infrastructures of the interoperability components are operated in accordance with this Regulation.

2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed referred to in Article 53(1).

3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, [ETIAS], SIS, and Eurodac, and [the ECRIS-TCN system], and the European search portal, the shared biometric matching service, the common identity repository and the multiple-identity detector.

   eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the SIS, Eurodac or [ECRIS-TCN system] deriving from the establishment of interoperability and provided for by this Regulation.

   eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5).

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

4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the Interoperability Advisory Group referred to in Article 65, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA and which will participate in the interoperability components.

5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.

   The Programme Management Board shall every month submit to the Management Board written reports on progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.

6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

(e) communication plans ensuring full information to non-participating Members of the Management Board.

The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, and Article 10 of the eu-LISA Rules of Procedure shall apply *mutatis mutandis*. eu-LISA shall provide the Programme Management Board with a secretariat.

The Interoperability Advisory Group referred to in Article 65 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.

Article 53
Responsibilities of eu-LISA following the entry into operations

1. Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical management of the central infrastructure and the national uniform interfaces. In cooperation with the Member States, it shall ensure at all times the best available technology, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.

Technical management of the interoperability components shall consist of all the tasks necessary to keep the interoperability components functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository in accordance with Article 37.

4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.

Article 54
Responsibilities of Member States

1. Each Member State shall be responsible for:

   (a) the connection to the communication infrastructure of the European search portal (ESP) and the common identity repository (CIR);

   (b) the integration of the existing national systems and infrastructures with the ESP, shared biometric matching service, the CIR and the multiple-identity detector;

   (c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;

   (d) the management of, and arrangements for, access by the duly authorised staff, and by the duly empowered staff, of the competent national authorities to the ESP, the CIR and the multiple-identity detector in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

   (e) the adoption of the legislative measures referred to in Article 20(3) in order to access the CIR for identification purposes;

   (f) the manual verification of different identities referred to in Article 29;

   (g) the implementation of data quality requirements in the EU information systems and in the interoperability components;

   (h) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).

2. Each Member State shall connect their designated authorities referred to in Article 4(24) to the CIR.

Article 54a
Responsibilities of Europol

1. Europol shall ensure processing of the queries by the ESP to the Europol data and shall accordingly adapt its Querying Europol Systems (QUEST) interface for basic protection level (BPL) data.

2. Europol shall be responsible for the management of, and arrangements for, its duly authorised staff to use and access respectively the ESP and the CIR in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles.

Article 55
Responsibilities of the ETIAS Central Unit

The ETIAS Central Unit shall be responsible for:

   (a) the manual verification of different identities referred to in Article 29;

   (b) carrying out a multiple-identity detection between the data stored in the VIS,

Eurodac and the SIS referred to in Article 59.

CHAPTER IX
Final provisions

Article 56
Reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the European search portal (ESP), solely for the purposes of reporting and statistics without enabling individual identification:

   (a) number of queries per user of the ESP profile;

   (b) – (not applicable).

2. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the common identity repository, solely for the purposes of reporting and statistics without enabling individual identification:

   (a) number of queries for the purposes of Articles 20, 21 and 22;

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

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

   (d) the number of searches conducted with and without biometric data.

3. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the multiple-identity detector, solely for the purposes of reporting and statistics without enabling individual identification:

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

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

   (b) the number of searches conducted with and without biometric data;

   (c) the number of each type of link.

4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[64] shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.

5. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository

[64] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on migration and security in the Union.

Article 57
Transitional period for the use of the European search portal

For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.

Article 58
Transitional period applicable to the provisions on access to the common identity repository for law enforcement purposes

Article 22 shall apply from the date of the start of operations referred to in Article 62(1).

Article 59
Transitional period for the multiple-identity detection

1. For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the multiple-identity detector (MID) and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the VIS, Eurodac and the SIS. The multiple-identity detections shall be carried out using only biometric data in accordance with Article 27(2) of this Regulation.

2. Where the query reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

   Where the query reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.

   Where several hits are reported, a link shall be created to each piece of data triggering the hit.

3. Where a yellow link is created in accordance with paragraph 3, the MID shall grant access to the identity data present in the different information systems to the ETIAS Central Unit.

4. Where a link is created to an alert in the SIS, other than a refusal of entry alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 24 of the Regulation on SIS in the field of border checks and Article 38 of the Regulation on SIS in the field of law enforcement respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.

6. eu-LISA shall assist where necessary the ETIAS Central Unit in carrying out the multiple-identity detection referred to in this Article.

Article 60
Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service, the common identity repository (CIR) and the MID shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.

   The following costs shall be excluded:

   (a) Member States' project management office (meetings, missions, offices);

   (b) hosting of national IT systems (space, implementation, electricity, cooling);

   (c) operation of national IT systems (operators and support contracts);

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

3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol, respectively.

Article 61
Notifications

1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.

   A consolidated list of those authorities shall be published in the *Official Journal of the European Union* within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 62. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.

2. eu-LISA shall notify the Commission of the successful completion of the test referred to in Article 62(1)(b).

3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.

4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.

Article 62
Start of operations

1. The Commission shall decide the date from which each interoperability component is to start operations, after the following conditions are met:

(a) the measures referred to in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, 19, 34 and 39 and have notified them to the Commission;

(d) the Member States have notified the Commission as referred to in Article 61(1);

(e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).

2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).

3. The Commission decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.

4. The Member States and Europol shall start using the interoperability components from the date determined by the Commission in accordance with paragraph 1.

Article 63
Exercise of the 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 Articles 8(2) and 9(7) shall be conferred on the Commission for an indeterminate period of time from [*the date of entry into force of this Regulation*].

3. The delegation of power referred to in Articles 8(2) and 9(7) 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 on Better Law-Making of 13 April 2016.

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

6. A delegated act adopted pursuant to Articles 8(2) and 9(7) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Article 64
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.

Article 65
Advisory group

An Advisory Group shall be established by eu-LISA in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.

Article 66
Training

eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.

Article 67
Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.

Article 68
Monitoring and evaluation

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

2. By [*Six months after the entry into force of this Regulation* — OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components. Once the development is finalised, a report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components.

4. Four years after the start of operations of each interoperability component and every four years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components, including the security thereof.

5. In addition, one year after each report from eu-LISA, the Commission shall produce an overall evaluation of the components, including:

   (a) an assessment of the application of this Regulation;

   (b) an examination of the results achieved against objectives and the impact on fundamental rights;

   (c) an assessment of the continuing validity of the underlying rationale of the interoperability components;

   (d) an assessment of the security of the interoperability components;

   (e) an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.

   The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[65]

6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the common identity repository for law enforcement purposes, containing information and statistics on:

   (a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;

   (b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by the Eurodac Regulation;

   (c) the number of requests for access to the common identity repository for law enforcement purposes;

   (d) the number and type of cases that have ended in successful identifications;

   (e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the *ex post* verification carried out by the central access point.

   Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

---

[65] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

Article 69
Entry into force and applicability

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

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

Done at Brussels,

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. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

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 impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on operational appropriations

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and the Council establishing interoperability between European Union information systems for security, border and migration management.

1.2. Policy area(s) concerned

Home Affairs (title 18)

1.3. Nature of the proposal/initiative

X The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[66]

☐ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objective(s)

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/initiative

Border management – saving lives and securing external borders

The interoperability components create the opportunity for a better use of the information contained in the existing EU systems for security, border and migration management. These measures mainly avoid that the same person is recorded in different systems with different identities. Currently, the unique identification of a person is possible within a given system but not across systems. This can lead to erroneous decisions by the authorities or conversely be used by male fide travellers to hide their real identity.

Better information exchange

The proposed measures also provide a streamlined but still delimited access of law enforcement services to these data. But, unlike today, there is one single set of conditions rather than a different set for accessing each data collection.

1.4.2. Specific objective(s) and Specific objective No [ ]

The establishment of the interoperability components has the following general objectives:

(a) to improve the management of the external borders;

(b) to contribute to preventing and combating irregular migration; and

[66] As referred to in Article 54(2)(a) or (b) of the Financial Regulation.

(c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States.

The objectives of ensuring interoperability shall be achieved by:

(a) ensuring the correct identification of persons;

(b) contributing to fighting identity fraud;

(c) improving and harmonising data quality requirements of the respective EU information systems;

(d) facilitating the technical and operational implementation by Member States of existing and future EU information systems;

(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems;

(f) simplifying and making more uniform the conditions for law enforcement access to the EES, the VIS, the ETIAS and Eurodac;

(g) supporting the purposes of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN System

ABM/ABB activity(ies) concerned

Chapter Security and Safeguarding Liberties: Internal Security

1.4.3. Expected result(s) and impact

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

The general objectives of this initiative result from the two Treaty-based goals:

1. To improve the management of the Schengen external borders, building on the European Agenda on Migration and subsequent communications, including the Communication on preserving and strengthening Schengen area.

2. To contribute to the internal security of the European Union, building on the European Agenda on Security and the Commission's work towards an effective and genuine Security Union.

The specific policy objectives of this interoperability initiative are:

The specific objectives of this proposal are to:

1. ensure that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast, seamless, systematic and controlled access to the information that they need to perform their tasks;

2. provide a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of bona fide persons and combating identity fraud;

3. facilitate identity checks of third-country nationals, on the territory of a Member State, by police authorities; and

4. facilitate and streamline access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.

To meet the specific objective 1, the European search portal (ESP) will be developed.

To meet the specific objective 2, the multiple identity detector (MID) will be put in place, supported by the common identity repository (CIR) and the shared biometric matching service (shared BMS).

To meet the specific objective 3, authorised officials will be granted access to the CIR for the purpose of identification.

To meet objective 4 the CIR will contain a hit-flag functionality which will allow for a two-step approach for law enforcement access to border management systems.

In addition to these four interoperability components the objectives described in section 1.4.2 will be furthermore be supported by the establishment and governance of the Universal Message Format (UMF) as an EU standard for the development of information systems in the area of justice and home affairs, and by the establishment of a common repository for reporting and statistics (CRRS).

1.4.4. Indicators of results and impact

Specify the indicators for monitoring implementation of the proposal/initiative.

Each of the measures proposed requires the development, followed by the maintenance and operations, of that component.

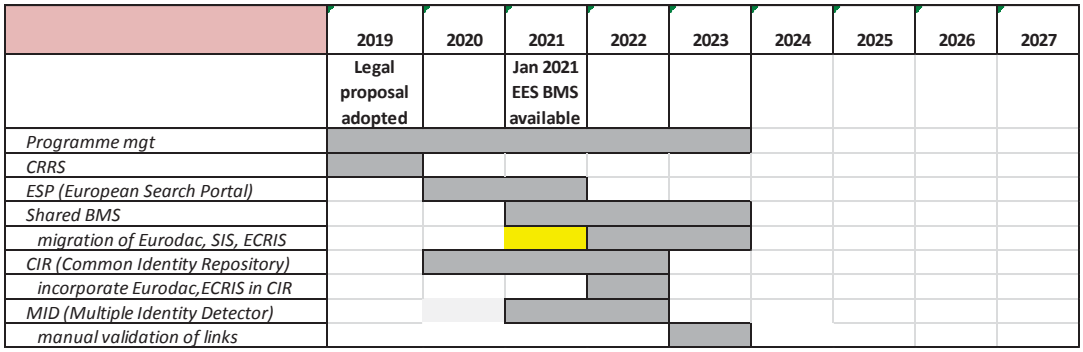
During the development

The development of each component will be done once the prerequisites are fulfilled i.e. the legal proposal is adopted by the co-legislators and the technical prerequisites fulfilled, as some components can only be built once another one is available.

Specific objective: ready for operations by the target due date

By the end of 2017, the proposal is sent to the co-legislators for their adoption. The assumption is made that the adoption process will be completed during 2018 by analogy with the time taken for other proposals.

Under that assumption, the start of the development period is set at the beginning of 2019 (= 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. On the other hand, the shared BMS needs to be available before the CIR and the MID can be completed. The durations of development are indicated on the chart below:



(Block in yellow relates to a specific Eurodac-related task.)

- Common repository for reporting and statistics (CRRS): due date: T0 + 12 months (2019-2020)

- European search portal (ESP): due date: T0+36 months (2019-2021)

- Shared biometric matching service (shared BMS) is first created for delivering the Entry/Exit System (EES). When this milestone is achieved, the applications that will use the shared BMS need to be updated and the data contained in the SIS automated fingerprint identification system (AFIS), the Eurodac AFIS and the data of ECRIS-TCN migrated into the shared BMS. The due date for completion is end-2023.

- The common identity repository (CIR) is first created during the implementation of EES. When the EES is completed, the data from Eurodac and ECRIS are incorporated into the CIR. The due date for completion is end-2022 (availability of shared BMS + 12 months).

- The multiple identity detector (MID) is created after the CIR is operational. The due date for completion is end-2022 (availability of shared BMS + 24 months) but there is a very resource-consuming period of validating links between identities that are proposed by the MID. Each of the estimated links needs to be manually validated. This takes till the end of 2023.

The period of operations starts once the development period indicated above is completed.

Operations

Indicators related to each specific objective mentioned under 1.4.3 are as follows:

1. Specific objective: Fast, seamless and systematic access to authorised data sources

- The number of use cases executed (= number of searches that can be handled by ESP) per time period.

- Number of searches handled by ESP compared with total number of searches (via ESP and systems directly) per time period.

2. Specific objective: Detect multiple identities

- The number of identities linked to the same set of biometric data compared with the number of identities with biographical information per time period.

- The number of detected cases of identity fraud compared with the number of linked identities and total number of identities per time period.

3. Specific objective: Facilitate identifications of third-country nationals

- The number of identification checks performed compared with total number of transactions per time period.

4. Specific objective: Simplify access to authorised data sources for law enforcement purposes

- The number of 'step 1' (= a data presence check) accesses for law enforcement purposes per time period.

- Number of 'step 2' (= the actual consultation of data from the EU systems within the scope) accesses for law enforcement purposes per time period.

5. Cross-cutting, additional objective: Improving the quality of data and the use of data for better policymaking

- The regular issuance of data quality monitoring reports.

- The number of ad hoc requests for statistical information per time period.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term

As demonstrated in the impact assessment that accompanies this legal proposal the respective proposed components are necessary to achieve interoperability:

- To meet the objective of providing authorised users with fast, seamless, systematic and controlled access to relevant information systems, a European search portal (ESP) should be created, built on a shared BMS to address all databases.

- To meet the objective of facilitating identity checks of third-country nationals, on the territory of a Member State, by authorised officers, a common identity repository (CIR) should be created, containing the minimum set of identification data, and built on the same shared BMS.

- To meet the objective of detecting multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud, a multiple identity detector (MID) should be built, containing links between multiple identities across systems.

- To meet the objective of facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems, for the purpose

of preventing, investigating, detecting or prosecuting serious crime and terrorism, a 'hit-flagging' functionality should be included in the common identity repository (CIR).

Since all objectives must be met, the complete solution is the combination of ESP, CIR (with hit flagging) and MID, all relying on the shared BMS.

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 that is additional to the value that would have been otherwise created by Member States alone.

Action is required at the European level because the systems that are proposed to be made interoperable are systems used by multiple Member States: either all Member States (in the case of Eurodac) or all Member States that are part of the Schengen area (for EES, VIS, ETIAS and SIS). By definition, action simply cannot be taken at another level.

The main expected added value is to eliminate the cases of identity fraud, map the cases where a person has used different identities to enter the EU, and avoid that *bona fide* persons are confused with *mala fide* persons with the same name. An additional added value is that the interoperability proposed here allows an easier implementation and maintenance of EU large-scale IT systems. For law enforcement services, the measures proposed should result in a more frequent and successful access to specific data within EU large-scale IT systems. At an operational level, the quality of data can only be maintained and improved if it is monitored. Further, for policymaking and decision-making, there is a need to make it possible to undertake *ad hoc* queries of anonymised data.

A cost-benefit analysis is part of the impact assessment and taking only those benefits that can be quantified, the expected benefits can reasonably be estimated at about € 77.5 million per year and accrue mainly to Member States. These benefits stem essentially from:

- Reduced cost of changes to national applications when the central system is operational (estimated at €6m per year for Member State IT departments);

- Cost saving of having one central shared BMS rather than one BMS per central system containing biometrics (estimated at €1.5m per year and a one-off saving of €8m for eu-LISA.

- Saved cost of identification of multiple identities compared with the situation where the same result would be achieved without the proposed means. This would represent a cost saving of at least €50m per year for Member State administrations for border management, migration and law enforcement.

- Saved training costs for a large end-user group compared with a situation where training is required on a recurrent basis, estimated at €20m per year for Member State administrations for border management, migration and law enforcement.

1.5.3. Lessons learned from similar experiences in the past

Experience with the development of the second generation Schengen (SIS II) and of the Visa Information System (VIS) showed the following lessons:

1. As a possible safeguard against cost overruns and delays resulting from changing requirements, any new information system in the area of freedom, security and justice, particularly if it involves a large-scale IT system, should not be developed before the underlying legal instruments setting out its purpose, scope, functions and technical details have been definitively adopted.

2. For SIS II and VIS, national development in Member States could be co-financed under the External Borders Fund (EBF) but this was not compulsory. Hence it was not possible to have an overview of the level of advancement in those Member States that had not provided for the respective activities in their multiannual programming or lacked precision in their programming. Therefore, it is now proposed that the Commission reimburses all integration costs incurred by Member States, so as to be able to monitor the advancement of these developments.

3. With a view to facilitating the general coordination of the implementation, all the proposed message exchanges between national and central systems will reuse existing networks and the national uniform interface.

1.5.4. Compatibility and possible synergy with other appropriate instruments

Compatibility with the current MFF

The ISF Borders Regulation is the financial instrument where the budget for implementation of the interoperability initiative has been included.

It provides in Article 5(b) that EUR 791 million is to be implemented through a programme for developing IT systems based on existing and/or new IT systems, supporting the management of migration flows across the external borders subject to the adoption of the relevant Union legislative acts and under the conditions laid down in Article 15. Of this EUR 791 million, EUR 480.2 million is reserved for the development of the EES, EUR 210 million for ETIAS and EUR 67.9 million for the revision of SIS II. The remainder (EUR 32.9 million) is to be reallocated using ISF-B mechanisms. The current proposal requires EUR 32.1 million for the current multiannual financial framework period which fits with the remaining budget.

The current proposal requires EUR 424.7 million budget in total (heading 5 included) over the period from 2019 till 2027. The current MFF only covers the two-year period for 2019 and 2020. Costs have however been estimated till 2027 included to give an informed view on the financial consequences of this proposal and without prejudging the next multiannual financial framework.

The budget requested over nine years amounts to € 424.7 million as the following items are also covered:

(1) EUR 136.3 million for Member States to cover the changes to their national systems in order to use the interoperability components, the NUI delivered by eu-LISA and a budget for the training of the substantial end-user community. There is no impact on current MFF as financing is provided from 2021 onwards.

(2) EUR 4.8 million for the EBCG Agency for hosting a team of specialists who during one year (2023) will validate the links between identities at the moment the MID goes live. The activities of the team can be associated with identity disambiguation as attributed to the EBCG Agency under the ETIAS proposal. There is no impact on current MFF as financing is provided from 2021 onwards.

(3) EUR 48.9 million for Europol to cover the upgrade of Europol's IT systems to the volume of messages to be handled and the increased performance levels. The interoperability components will be used by ETIAS in order to consult the Europol data. However the current information handling capacity of Europol is not compliant with the substantial volumes (average of 100,000 queries per day) and shortened response time. EUR 9,1 million is spent on current MFF.

(4) EUR 2.0 million for CEPOL to cover the preparation and delivery of training to operational staff. EUR 0,1 million is scheduled in 2020.

(5) EUR 225.0 million for eu-LISA which covers the total cost for the development of the programme delivering the five interoperability components (€ 68.3 million), the maintenance cost from the moment components are delivered up until 2027 (€ 56.1 million), a specific budget of € 25.0 million for the migration of data from existing systems to the shared BMS and the additional costs for the NUI update, network, training and meetings. A specific budget of € 18.7 million covers the cost of upgrading and operating ECRIS-TCN in high-availability mode from 2022. Out of the total amount, EUR 23.0 million is spent during the current MFF.

(6) EUR 7.7 million for DG HOME in order to cover a limited increase of staff and related costs during the development period of the different components, as the Commission will also take the responsibility for the committee dealing with UMF (Uniform Message Format). This budget which falls under heading 5 is not to be covered by the ISF budget. For information EUR 2,0 million are due over the period 2019-2020.

Compatibility with previous initiatives

This initiative is compatible with the following:

In April 2016, the Commission presented a **Communication *Stronger and smarter information systems for borders and security*** to address a number of structural shortcomings related to information systems. Three actions arose from this:

First, the Commission took **action to strengthen and maximise the benefits of existing information systems**. In December 2016, the Commission adopted proposals for the further reinforcement of the existing Schengen Information System (SIS). In the meantime, following the Commission's proposal of May 2016, negotiations were accelerated on the revised legal basis for Eurodac — the EU asylum fingerprint database. A proposal for a new legal basis for the Visa Information System (VIS) is also under preparation, and will be submitted in the second quarter of 2018.

Second, the Commission proposed **additional information systems to address identified gaps** in the EU's data management architecture. Negotiations on the Commission's April 2016 proposal to establish an Entry/Exit System (EES)[67] — to improve border check procedures for non-EU nationals travelling to the EU — were concluded as early as July 2017, when the co-legislators reached a political agreement, confirmed by the European Parliament in October 2017 and formally adopted by the Council in November 2017. In November 2016, the Commission also presented a proposal for the establishment of a European Travel Information and Authorisation System (ETIAS)[68]. This proposal aims to strengthen security checks

67 COM(2016)194 of 6 April 2016

68 COM(2016)731 of 16 November 2016

on visa-free travellers by enabling advance irregular migration and security checks. It is currently under negotiation by the co-legislators. In June 2017, the European Criminal Record Information System for third-country nationals (ECRIS-TCN system)[69] was also proposed to address the gap identified with regards to exchange of information between Member States on convicted non-EU nationals

Third, the Commission worked **towards the interoperability of information systems**, focusing on the four options presented in the April 2016 Communication[70] to achieve interoperability. Three of the four options are precisely the ESP, the CIR and the shared BMS. It became clear afterwards a distinction had to be made between the CIR as the database of identities and a new component that identifies multiple identities linked to a same biometric identifier (MID). So the four components are now: the ESP, the CIR, the MID and the shared BMS.

Synergy

Synergy is understood here as the benefit realised by reusing existing solutions and avoiding new investments all the way around.

A major synergy exists between these initiatives and the development of the EES and ETIAS.

For the functioning of the EES, an individual file is created for all third-country nationals entering the Schengen area for a short stay. For this purpose, the current biometric matching system used for VIS, containing the fingerprint templates for all visa-required travellers, will be extended to also include the biometrics from visa-exempt travellers. The shared BMS is thus conceptually a further generalisation of the biometrics matcher that will be built as part of the EES. The biometric templates contained in the biometric matcher of SIS and Eurodac will then be migrated (this is the technical term when data are moved from one system to another) to that shared BMS. According to supplier data, the storage in separate databases costs on average 1 euro per biometric set (there are potentially 200 million data sets in total) while the average cost drops to €0.35 per biometric set when a shared BMS solution is created. The higher costs on the hardware required for a high volume of data partly offsets these benefits but in the end the cost of a shared BMS is estimated to be 30% lower than when the same data are stored in multiple smaller BMS systems.

For the functioning of ETIAS, a component needs to be available for querying a set of EU systems. Either the ESP is used or a specific component is built as part of the ESP proposal. The interoperability proposal enables the building of one component rather than two.

There is also a synergy achieved by reusing the same national uniform interface (NUI) that is used for EES and ETIAS. The NUI will need to be updated but will continue to be used.

69 COM(2017)344 of 29 June 2017
70 COM(2016)205 of 6 April 2016

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

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

– ☐ Financial impact from YYYY to YYYY

☒ Proposal/initiative of **unlimited duration**

– Development period from 2019 to 2023 included, followed by full-scale operations.

– Duration of the financial impact is therefore provided for 2019 to 2027.

1.7. Management mode(s) planned[71]

☒ **Direct management** by the Commission

– X 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 208 and 209 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

Blocks	Development phase	Operations phase	Management mode	Actor
Development and maintenance (of interoperability components for the central systems, system training)	X	X	Indirect	eu-LISA Europol CEPOL

[71] 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.

Blocks	Development phase	Operations phase	Management mode	Actor
Data migration (migration of biometric templates to a shared BMS), network costs, NUI update, meetings and training	X	X	Indirect	eu-LISA
Validation of links when creating MID	X	-	Indirect	EBCG
Customisation of NUI, integration of national systems and end-user training	X	X	Shared (or direct) (1)	COM + Member States

(1) There are no amounts for the operations phase included in this instrument.

The development period starts from 2019 and lasts till the delivery of each component, running from 2019 to 2023 (see Section 1.4.4).

1. Direct management by DG HOME: During the development period, if necessary, actions may also be implemented directly by the Commission. This could include, in particular, Union financial support for activities in the form of grants (including to Member State national authorities), public procurement contracts and/or reimbursement of costs incurred by external experts.

2. Shared management: During the development phase, Member States will be required to adapt their national systems in order to access the ESP rather than individual systems (this is for the outgoing messages from Member States) and for changes to the answers of their search requests (the incoming messages towards Member States). An update of the existing NUI implemented for EES and ETIAS will also be performed.

3. Indirect management: eu-LISA will cover the development part of all IT strands of the project, i.e. the interoperability components, the update of the national uniform interface (NUI) in each Member State, the update of the communication infrastructure between the central systems and the national uniform interfaces, the migration of biometric templates from the existing biometric matching systems of SIS and Eurodac to the shared BMS and the data cleansing activity that goes with this.

During the period of operations, eu-LISA will execute all technical activities linked to the maintenance of the components.

The European Border and Coast Guard (EBCG) Agency will incorporate an additional team dedicated to the validation of links once the MID is put into operation. This is a task limited in duration.

Europol will cover the development and maintenance of its systems to ensure interoperability with ESP and ETIAS.

CEPOL prepares and delivers the training to operational services following a train-the-trainers approach.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The monitoring and reporting rules for the development and maintenance of other systems:

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

2. Within six months after the entry into force of this Regulation and every six months thereafter during the development phase of the components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of each component. Once the development is finalised, a report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved, as well as justifying any divergences.

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the components.

4. Four years after the start of operations of the last component implemented and every four years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the components.

5. Five years after the start of operations of the last component implemented and every four years thereafter, the Commission shall produce an overall evaluation and make any necessary recommendations. This overall evaluation shall include: the results achieved by the components having regard to its objectives of interoperability, maintainability, performance and financial implications, and the impact on fundamental rights.

The Commission shall transmit the evaluation report to the European Parliament and the Council.

6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5 according to the quantitative indicators predefined by the Commission and/or eu-LISA. This information shall not jeopardise working methods or include information that reveals sources, identities of staff members or investigations of the designated authorities.

7. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.

8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to EU systems for law enforcement purposes containing information and statistics on:

- the exact purpose of the consultation including the type of terrorist or serious criminal offence;

- reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;

- the number of requests for access to the components for law enforcement purposes;

- the number and type of cases that have ended in successful identifications;

- the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

Member State and Europol's annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

2.2. Management and control system

2.2.1. Risk(s) identified

The risks are the ones related to an IT development of five components by an external contractor managed by eu-LISA. These are typical project risks:

1. The risk of not completing the project on time;

2. The risk of not completing the project within budget;

3. The risk of not delivering the full scope of the project.

The first risk is the most important one as an overrun in time leads to higher costs as most costs have a relationship to duration: staff costs, licence costs paid per year, etc.

These risks can be mitigated by applying project management techniques, including contingency in development projects and staffing sufficiently in order to be able to absorb peaks of work. Estimation of effort is indeed usually done by assuming an even workload spread over time while the reality of projects is of uneven workloads that are absorbed by higher resource allocations.

There are several risks related to the use of an external contractor for this development work:

1. in particular, the risk that the contractor fails to allocate sufficient resources to the project or that it designs and develops a system that is not state of the art;

2. the risk that administrative techniques and methods to handle large-scale IT projects are not fully respected as a way of reducing costs by the contractor;

3. finally, the risk of the contractor facing financial difficulties for reasons external to this project cannot be entirely excluded.

These risks are mitigated by awarding contracts on the basis of strong quality criteria, checking references of contractors and maintaining a strong relationship with them. Finally, as a last resort, strong penalty and termination clauses can be included and applied when required.

2.2.2. Information concerning the internal control system set up

eu-LISA is meant to be a centre of excellence in the field of development and management of large-scale IT systems. It shall execute the activities linked to the

development and the operations of the different interoperability components including the maintenance of the national uniform interface in the Member States.

During the development phase, all development activities will be executed by eu-LISA. This will cover the development part of all strands of the project. The costs related to the integration of systems in Member States during development will be managed by the Commission via shared management or grants.

During the operational phase, eu-LISA will be responsible for the technical and financial management of the components used centrally, notably the award and management of contracts. The Commission will manage the funds to Member States for the expenses for national units via the ISF/Borders (national programmes).

In order to avoid delays at national level, an efficient governance between all stakeholders is to be planned prior to the start of the development. The Commission assumes an interoperable architecture to be defined at the beginning of the project in order to be applied in the EES and ETIAS projects, as these projects deliver and use the shared BMS, the common identity repository and the European search portal. A member of the project management team of the interoperability project should be part of the project governance structure of EES and ETIAS.

2.2.3. Estimate of the costs and benefits of the controls and assessment of the expected level of risk of error

There is no estimate provided, as the control and mitigation of risks is an inherent task of the project governance structure.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

The measures envisaged to combat fraud are laid down in Article 35 of Regulation (EU) 1077/2011, which provides as follows:

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EC) No 1073/1999 shall apply.

2. The Agencies shall accede to the Interinstitutional Agreement concerning internal investigations by the European Anti-Fraud Office (OLAF) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agencies.

3. The decisions concerning funding and the implementing agreements and instruments resulting from them shall explicitly stipulate that the Court of Auditors and OLAF may carry out, if necessary, on-the-spot checks among the recipients of the Agencies' funding and the agents responsible for allocating it.

In accordance with this provision, the decision of the Management Board of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Union's interests was adopted on 28 June 2012.

DG HOME's fraud prevention and detection strategy will apply.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

THE ESTIMATED IMPACT ON EXPENDITURE AND STAFFING FOR THE YEARS 2021 AND BEYOND IN THIS LEGISLATIVE FINANCIAL STATEMENT IS ADDED FOR ILLUSTRATIVE PURPOSES AND DOES NOT PREJUDGE THE NEXT MULTIANNUAL FINANCIAL FRAMEWORK

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 [Heading……...……]	Diff./Non-diff.[72]	from EFTA countries [73]	from candidate countries[74]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
3	18.02.01.03 – Smart Borders	Diff	No	No	Yes	No
3	18.02.03 – European Border and Coast Guard Agency (Frontex)	Diff	No	No	Yes	No
3	18.02.04 – EUROPOL	Diff	No	No	No	No
3	18.02.05 - CEPOL	Non-diff	No	No	No	No
3	18.02.07 – European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)	Diff	No	No	Yes	No

72 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

73 EFTA: European Free Trade Association.

74 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

[This section should be filled in using the **spreadsheet on budget data of an administrative nature** (second document in annex to this financial statement) and uploaded to DECIDE for interservice consultation purposes.]

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	3	Security and Citizenship

DG Home			Year **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Year 2028**	**TOTAL**
• Operational appropriations													
18.02.01.03 – Smart Borders	Commitments	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Payments	(2.	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Appropriations of an administrative nature financed from the envelope of specific programmes[75]													
Number of budget line		(3)											
TOTAL appropriations for DG Home	Commitments	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Payments	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

The expenditures will cover costs related to:

[75] 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.

– The cost for adapting the NUI (national uniform interface) whose development is financed under the EES proposal, a budgeted amount for the changes to the systems in the Member States in order to take into account the modifications of the central systems and a budgeted amount for end-user training.

18.0203 – EBCG			Year **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Title 1: Staff expenditures	Commitments	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Payments	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Title 2: Infrastructure and Operating expenditure	Commitments	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Payments	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Title 3: Operational expenditure	Commitments	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Payments	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTAL appropriations for Europol	(Total commitments = Total payments)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– The budget for the EBCG covers the expenditures of a team dedicated for the validation of links generated by the MID (multiple identity detector) on the legacy data (something like 14 million records). The volume of links to be validated manually is estimated around 550.000. The dedicated team set up for this purpose is added to the EBCG team set up for ETIAS because this is functionally close and avoids the set-up costs of a new team. The work is expected to take place in 2023. The contract agents are therefore recruited up to 3 months in advance and their contract stopped up to 2 months after the end of the migration activity. Another part of the required resources are not assumed to be recruited as contract agents and will be hired in as consultants. This explains the costs under Title 3 for 2023. They are assumed to be hired one month in advance. Further details on staff levels are provided later.

– Title 1 includes therefore the cost of 20 internal staff, and the provisions for a strengthening of the management and support staff.

– Title 2 includes the additional cost for hosting the 10 additional contractor's staff.

– Title 3 includes the fee for the additional 10 contractor's staff. There are no other types of cost included.

18.0204 - Europol			Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
Title 1: Staff expenditures	Commitments	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Payments	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Title 2: Infrastructure and Operating expenditure	Commitments	(1a)	0	0	0	0	0	0	0	0	0	0
	Payments	(2a)	0	0	0	0	0	0	0	0	0	0
Title 3: Operational expenditure	Commitments	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Payments	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTAL appropriations for Europol	(Total commitments = Total payments)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Europol's expenditures will cover the upgrade of Europol's ICT systems capabilities to deal with the volume of messages to be handled, and the required increased performance levels (response time).

Title 1 Staff expenditure covers the costs related to additional ICT staff to be recruited to reinforce Europol information systems for the reasons described above. Further details regarding the division of posts between temporary agents and contract agents, and their expertise are provided below.

Title 3 includes costs for the hardware and software needed to reinforce Europol information systems. At present, Europol's IT systems serve a limited designated community of Europol, Europol Liaison Officers and investigators in the Member States who use these systems for analytical and investigative purposes. With the implementation of QUEST (the system interface that will allow the ESP to query Europol data) at basic protection level (currently Europol information systems are accredited up to EU restricted and EU confidential level), Europol information systems will be made available to a much larger authorised law enforcement community. In addition to these increases, ESP will be used by ETIAS to automatically query Europol data to process travel authorisations. This will increase the volume of queries against Europol data from approximately 107 000 queries per month at present, to more than 100 000 queries per day, and will also require 24/7 availability of Europol information systems and very short response times to meet the requirements imposed by the ETIAS Regulation. The majority of the costs are limited to the period before the interoperability components become operable, but some ongoing commitments are needed to ensure high and continuous availability of Europol information systems. Also, some development works are needed to implement interoperability components by Europol as a user.

18.0205 - CEPOL			Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
Title 1: Staff expenditures	Commitments	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Payments	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Title 2: Infrastructure and Operating expenditure	Commitments	(1a)	0	0	0	0	0	0	0	0	0	0
	Payments	(2a)	0	0	0	0	0	0	0	0	0	0
Title 3: Operational expenditure	Commitments	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Payments	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTAL appropriations for CEPOL	(Total commitments = Total payments)	=1+1a +3a	0	0,144	0.384,	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Centrally coordinated EU level training improves coherent implementation of training courses at national level and as a consequence ensures correct and successful implementation and use of interoperability components. CEPOL — as the EU Agency for Law Enforcement Training — is well-positioned to deliver central EU level training. These expenditures cover the preparation of the 'training for Member State trainers' required to use the central systems once they are made interoperable. The costs include those related to a small personnel increase for CEPOL to coordinate, manage, organise and update the courses and the cost for delivering a number of training sessions per year and preparing the online course. Details of these costs are explained below. The training effort is concentrated on the periods immediately preceding go-live. A continuous effort remains necessary beyond the go-live as the interoperable components are maintained and the trainers do not permanently remain the same persons, based on the experience of delivering existing training on Schengen information system.

18.0207 - eu-LISA			Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
Title 1: Staff expenditures	Commitments	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Payments	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344

Title 2: Infrastructure and Operating expenditure	Commitments	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Payments	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Title 3: Operational expenditure	Commitments	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Payments	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTAL appropriations for eu-LISA	(Total commitments = Total payments)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

These expenditures will cover:

– The development and maintenance of the four interoperability components (European search portal (ESP), shared biometric matching service (shared BMS), common identity repository (CIR), and multiple identity detector (MID) included in the legal proposal plus the common repository for reporting and statistics (CRRS). eu-LISA will act as the representative of the project owner and use its own staff for drafting specifications, selecting contractors, directing its work, submitting results to a set of tests and accepting the work done.

– The costs involved with the data migration of legacy systems to the new components. eu-LISA has no direct role however in the initial data load for the MID (the validation of links) because this is an action on the data content itself. The migration of biometric data of legacy systems deals with the format and the label of data and not the data content.

– The costs for upgrading and operating ECRIS-TCN to a high availability system from 2022. ECRIS-TCN is the central system containing the criminal records of third-country nationals. The system is planned to become available by 2020. The interoperability components are expected to also access that system which should therefore also become a high availability system. The operational expenditures include the additional cost for achieving that high availability. There is a significant development cost in 2021 followed by an on-going maintenance and operations cost. These costs are not included in the Legislative Financial Sheet of the revision of the founding regulation of eu-LISA[76] which only includes budgets from 2018 till 2020 and therefore does not overlap with this budget request.

[76] COM 2017/0145 (COD) Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011

– The pattern of expenditure is the result of the project sequencing. As the different components are not independent from one another, the development period spans from 2019 to 2023. However from 2020, maintenance and operations on the first available components already start. This explains why expenditures start slowly, increase and then diminish to a constant value.

– The expenditures under title 1 (staff expenditure) follow the project sequencing: more staff are required to deliver the project with the contractor (whose expenses are under title 3). When the project is delivered, part of the delivery team is assigned to evolution and maintenance work. At the same time, staff for operating the newly delivered systems increases.

– The expenditure under title 2 (infrastructure and operating expenditure) covers the additional office space for the temporary hosting of the contractor teams in charge of the development, maintenance and operations tasks. The pattern over time of the expenditure is therefore also following the evolution of staff levels. The costs for hosting additional equipment have already been included in the eu-LISA budget. There are also no additional costs for hosting eu-LISA staff as this is included in the standard staff cost.

– The expenditure under title 3 (operational expenditure) includes the cost for the contractor for developing and maintaining the system, the acquisition of the specific hardware and software.
The contractor costs start initially with the studies for specifying the components and the development only starting for one component (the CRRS). Over the period 2020-2022, costs then increase as more components are being developed in parallel. The costs do not decrease after the peak because the data migration tasks are particularly heavy in this project portfolio. The contractor costs then decrease as components are delivered and enter operations mode, which requires a stable resource pattern.
Simultaneously with the expenses under title 3, expenditure in 2020 increases strongly compared with the previous year because of the initial investment for hardware and software necessary during development. The expenses under title 3 (operational expenses) have an upsurge in 2021 and 2022 because the hardware and software investment costs for the operational IT environments (production and pre-production both for central unit and back-up central unit) are incurred in the year before go-live, respectively for interoperability components (the CIR and the MID) with high requirements on software and hardware. Once in operation, costs for hardware and software are essentially maintenance costs.

– More details are given further.

Heading of multiannual financial framework	5	'Administrative expenditure'

EUR million (to three decimal places)

		Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
DG HOME											
• Human resources Number of budget line 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Other administrative costs (meetings, etc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAL DG HOME	Appropriations	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

EUR million (to three decimal places)

		Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	Year 2028	TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Payments	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Estimated impact on operational appropriations

3.2.2.1. Estimated impact on EBCG Agency's appropriations

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

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
EBCG Agency ⇩	Type [77]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 [78] Validation of links																						
Nbr of staff recruited as experts to validate links	Contractor costs	0	0	0	0	0	0	0.8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Subtotal for specific objective No 1		**0**	**0**	**0**	**0**	**0**	**0**	**0.8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

These expenditures will cover:

- The recruitment of a sufficient additional manpower (estimate of about 10 experts) to the existing internal staff (estimated at about 20 persons) who will be hosted in the EBCG in order to validate links. There is only one month of recruitment before the start date planned to reach the required staffing levels.

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

[78] As described in point 1.4.2. 'Specific objective(s)…'

- There are no other contractor costs estimated. The software required is part of the shared BMS licence costs. There is no specific hardware processing capacity. The contractor personnel are assumed to be hosted by EBCG. It is therefore that, under Title 2 expenses, the annual cost of 12 square metres is added on average per person.

3.2.2.2. Estimated impact on Europol's appropriations

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

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
Europol ⇩	Type [79]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 [80] Development and Maintenance of (Europol) systems																						
IT environment	Infrastructure					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
IT environment	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
IT environment	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

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

[80] As described in point 1.4.2. 'Specific objective(s)…'

Development works	Contractor				0,360		0,360												0,720
Subtotal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

These expenditures will cover the need to reinforce Europol information systems and infrastructure to accommodate the increase of queries. These costs include:

– upgrading the security and network infrastructure, hardware (servers, storage) and software (licences). These upgrades need to be finalised before the European search portal and ETIAS become operable in 2021, the costs have been distributed equally between 2020 and 2021. As from 2022, the annual maintenance rate 20% has been taken as basis to calculate the maintenance costs. In addition, the standard five-year cycle to replace outdated hardware and infrastructure has been taken into account.

– Contractor costs for development works to implement QUEST in basic protection level.

3.2.2.3. Estimated impact on CEPOL's appropriations

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

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs **CEPOL** ⇩			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
	Type [81]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[82] Development and delivery of training courses																						
Number of residential courses	0,34 per course		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Online training	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Subtotal				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

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

[82] As described in point 1.4.2. 'Specific objective(s)…'

To ensure uniform implementation and use of the interoperability solutions, the training will be organised both centrally at EU level by CEPOL and by Member States. The expenditure for training at EU level includes:

– development of common curriculum to be used by Member States when implementing national training;

– residential activities to train the trainers. In the two years, immediately after the interoperability solutions become operational, the training is expected to be implemented on a larger scale and later maintained by two residential training courses per year.

– online course to complement the residential activities at EU level and in Member States.

3.2.2.4. Estimated impact on eu-LISA's appropriations

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

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
Eu-LISA ⇩	Type [83]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 [84] Development of Interoperability Components																						
Systems built	Contractor			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Software products	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Hardware products	Hardware			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
IT training	Training & other			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340
Subtotal for specific objective No 1				**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

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

[84] As described in point 1.4.2. 'Specific objective(s)…'

– This objective only includes the costs for delivering the four interoperability components and the CRRS.

– The costs for the shared BMS have been estimated taking into account the assumption that the EES that is about to be developed will serve as the core system for the development. Therefore, it is planned to reuse the biometric software licences (€36 million) included for EES.

– In this budget, the shared BMS is budget-wise treated as a further extension of the BMS for the EES. Therefore the current financial sheet includes the marginal cost for software licences (€ 6,8 million) for adding the approximately 20 million biometric data sets contained in the SIS AFIS (AFIS is the automated fingerprint identification system = the 'BMS' of SIS), the Eurodac AFIS and the future ECRIS-TCN (European Criminal Records Information System for third-country nationals) to the BMS delivered for EES. The costs for integrating the different systems (SIS, Eurodac, ECRIS-TCN) to the shared BMS are included in this financial sheet.

– As part of the work over 2019 and 2020, eu-LISA will be asked to work out the precise technical solution that cannot be defined at the time of submitting the legal proposal and to estimate the cost consequences for implementing the preferred technical solution. This may require a change to the cost estimate provided here.

– All components are delivered by the end of 2023, which explains why the contractor expenses reduce to close to zero by that time. Only a residual amount for recurrent update of the CRSS remains.

– Over the period 2019 to 2021, the expenses on software increase substantially as the software licence costs are incurred for the different environments needed for production, pre-production and testing and this both on central site and the back-up site. In addition, some specific and indispensable software components are priced according to the number 'referenced objects' (say the volume of data). As the database will ultimately contain about 220 million identities, the software price is proportionate to this value.

Indicate objectives and outputs Eu-LISA ⇩			Year 2019		Year 2020		Year 2021		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
	Type [85]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 2 Maintenance and operations of Interoperability Components																						
Systems kept operational	Contractor			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Software products	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Hardware products	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
IT training	Training			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotal for specific objective No 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Maintenance starts as soon as some components are delivered. Therefore the budget for a maintenance contractor is included from the moment the ESP is delivered (in 2021). The maintenance budget increases as more components are delivered and then reaches a more or less constant value representing a percentage (between 15 and 22%) of the initial investment

– Maintenance for hardware and software starts from the year of entry into operations: the evolution of the costs is similar to that for contractor costs.

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

Indicate objectives and outputs Eu-LISA ⇩			Year 2019		Year 2020		Year 2021		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
	Type [86]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 3 [87] Data migration																						
BMS legacy data migrated	To shared BMS			0		0		0		7,000		3,000		0		0		0		0		10,000
EDAC legacy data enabled for migration	EDAC redesign and rebuild			0		0		7,500		7,500				0		0		0		0		15,000
Subtotal for specific objective No 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– In the case of the shared BMS project, data need to be migrated from the other biometric engines to the shared BMS as this common system is operationally more effective and also gives a financial advantage compared with a situation where multiple smaller BMS systems would continue to be maintained.

– The current business logic of Eurodac is not clearly separated from the biometrics matching mechanism as is the case with the BMS operating with VIS. The internal functioning of Eurodac and the mechanism with which the business services call the underlying biometric matching services is a black box for the outside viewer and is based on proprietary technology. It will not be possible to simply migrate the data to a shared BMS and keep the existing business layer. Therefore the migration of data is accompanied by significant costs for changing the exchanging mechanisms with the Eurodac central application.

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

[87] As described in point 1.4.2. 'Specific objective(s)…'

Indicate objectives and outputs Eu-LISA ⇩			Year 2019		Year 2020		Year 2021		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
	Type[88]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 4[89] Network																						
Network connections	Network set-up			0		0		0		0,505										0		0,505
Network traffic handled	Network operations			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotal for specific objective No 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– The interoperability components only have a marginal effect on network traffic. In terms of data, only links between existing data are created which is a low-volume item. The cost included here is only the marginal increase of budget required on top of EES and ETIAS budgets for network set-up and traffic.

Indicate objectives and outputs			Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL

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

[89] As described in point 1.4.2. 'Specific objective(s)…'

Eu-LISA ⇩	Type [90]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 5 [91] Update NUI																						
NUI updated	Contractor			0		0		0		0,505		0,505										0		1,010
Subtotal for specific objective No 5				**0**		**0**		**0**		**0,505**		**0,505**												**1,010**

– The EES proposal introduced the concept of the national uniform interface (NUI) to be developed and maintained by eu-LISA. The table above contains the budget for updating the NUI for an additional type of information exchange. There is no additional cost on the operations of the NUI, which were already budgeted under the EES proposal.

Indicate objectives and outputs			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
Eu-LISA ⇩	Type [92]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 6: Meetings and training																						

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

[91] As described in point 1.4.2. 'Specific objective(s)…'

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

Monthly Progress meetings (Develop-ment)	0,021 per meeting x 10 per year	10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Quarterly meetings (operations)	0,021 x 4 per year	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Advisory Groups	0,021 x 4 per years	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
MS Training	0,025 per training	2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotal for specific objective No 6		20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

– The subtotal 6 includes the costs for organising meetings by the Management Authority (in this case eu-LISA) for the project governance. These are the costs for additional meetings for the delivery of the interoperability components.

– The subtotal 6 includes the costs for meetings of eu-LISA with Member State staff dealing with the development, maintenance and operations of the interoperability components and with organising and delivering training for Member State IT staff.

– During development, the budget includes 10 project meetings per year. Once operations are being prepared (and this is the case from 2019 onwards), four meetings are organised per year. At a more senior level, an Advisory Group is set up from the beginning to implement the Commission's implementing decisions. There are four meetings per year planned, as for the existing Advisory Groups. Further, eu-LISA prepares and delivers training for the IT staff in Member States. This is training on technical aspects of the interoperability components.

Indicate objectives and outputs Eu-LISA ⇩			Year 2019		Year 2020		Year 2021		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
	Type [93]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 7 [94] High availability of ECRIS-TCN																						
High available system	System set-up			0		0		8,067												0		8,067
High availability operations	System maintained and operated			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotal for specific objective No 4				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– The objective 7 is to move ECRIS-TCN from a system with a 'standard' availability to a high availability system. In 2021, ECRIS-TCN would undergo that upgrade which requires the acquisition of additional hardware essentially. Since ECRIS-TCN is planned to be completed in 2020, it is tempting to build that system as a high-available system from the start and integrated with the interoperability components. However given that many projects become dependent from one another it is cautious not making this assumption and budgeting separate actions. This budget is an additional budget to the cost for developing, maintaining or operating ECRIS-TCN in 2019 and 2020.

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

[94] As described in point 1.4.2. 'Specific objective(s)…'

3.2.2.5. Estimated impact on DG Home's appropriations

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

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs **DG Home** ⇩			Year **2019**		Year **2020**		Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
	Type 95	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1: Integration of (Member State) national systems																						
NUI ready for use	Customisation NUI - developments						30	3,150	30	3,150											30	6,300
MS systems adapted for interoperability	Integration costs						30	40,000	30	40,000	30	40,000									30	120,000
End-users trained	10.000 end—user sessions in total @ €1000 per session								5000	5,000	5000	5,000									10.000	10,000

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

Subtotal for specific objective No 1						**43,150**		**48,150**		**45,000**										**136,300**

– Specific Objective 1 deals with the funds made available to Member States in order to take the benefit of interoperable central systems. The NUI is customised both when ESP is implemented and when MID becomes operational. Each Member State then has a relatively moderate change (estimated at 150 man-days) to perform in order to adapt to these updated message exchanges with the central systems. More substantial is the change to the contents of the data that interoperability will introduce and which is covered under the 'integration cost'. These funds deal with changes to the sort of messages sent to the central system and for handling the returned answer. For estimating the costs of these changes, a budget of €4 million is allocated per Member State. This amount is the same as for the EES as there is a comparable amount of work required to adapt integration of national systems with NUI.

– The end-users need to be trained for the systems. This training for a very large end-user population is to be financed on the basis of €1,000 per session of 10 to 20 end-users for the estimated 10.000 sessions to be organised by all Member States in their own premises.

3.2.3. Estimated impact on human resources

3.2.3.1. EBCG Agency 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Officials (AD Grades)										
Officials (AST grades)	0									
Contract staff	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Temporary staff	0	0	0	0	0	0	0	0	0	0
Seconded National Experts										
TOTAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

The expected work to be carried out by these additional staff to the EBCG is limited in time (2023), more precisely starting 24 months after the availability date of the biometric engine for EES is available). However staff need to be recruited in advance (an average of three months is calculated) which explains the value in 2022. The work done is followed by wrap-up/termination tasks during two months, which explains the staff level in 2024.

The staff level itself is based on 20 persons required for the work to be done (plus 10 persons provided by a contractor and which is reflected in Title 3). The tasks are also assumed to happen over extended working hours and not being limited to standard business hours. Support and managerial staff are assumed to be provided relying on the resources of the Agency.

The staff number is based on the assumption that about 550.000 fingerprints will have to be assessed taking on average 5 to 10 minutes per case (17.000 prints per year checked).[96]

[96] Staff in 2020 and later years is indicative and will need to be assessed whether it is additional to the forecast of EBCG staff set out in COM(2015)671 or not

Number of staff	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Staff for processing links and decisions manually	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Title 1 - CA	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Title 1 - TA	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total Title 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Europol 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Officials (AD Grades)										
Officials (AST grades)	0									
Contract staff	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Temporary staff	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Seconded National Experts										
TOTAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

These costs are estimated on the basis of the following staff levels:

Number of FTEs for ICT	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**total**
Contract Staff	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Temporary staff	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Total Staff (FTEs)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Additional ICT staff for Europol is envisaged to reinforce Europol information systems in order to accommodate the increased number of queries from ESP and ETIAS and later to maintain the systems 24/7.

– For the ESP implementation phase (in 2020 and 2021) there is an additional need for technical experts (architects, engineers, developers, testers). Reduced number of technical experts will be needed for the years 2022 onwards to implement the rest of interoperability components and maintain the systems.

– As from second half of 2021, 24/7 ICT system monitoring needs to be implemented to ensure service levels of ESP and ETIAS. This will be done by 2 contract agents, working in 4 shifts 24/7.

– To the extent possible, the profiles have been divided between temporary agents and contract agents. It has to be noted though that due to high security requirements, in several posts it is possible to use temporary agents only. The request for Temporary Agents will take into account the results of the conciliation on the 2018 budget procedure.

3.2.3.3. CEPOL 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Officials (AD Grades)										
Officials (AST grades)										
Contract staff			0,070	0,070						**0,140**
Temporary staff		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Seconded National Experts										
TOTAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Additional staff is required as the training for Member State trainers needs to be developed specifically in view of using the interoperability components in operational circumstances.

- The development of curriculum and training modules should start at least 8 months before the system is operational. In the first two years after becoming operational, the training is at

its most intense. However, it needs to be maintained for a longer period to ensure coherent implementation, based on the experience with the Schengen information system.

- The additional staff is needed to prepare, coordinate and implement the curriculum, residential courses and online course. These courses can only be implemented in addition to CEPOL's existing training catalogue, and therefore additional staff are needed.

- It is planned to have one course manager as temporary agent throughout the development and maintenance period who will be supported by one contract agent in the most intense training organisation period.

3.2.3.4. Eu-LISA 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Officials (AD Grades)										
Officials (AST grades)										
Contract staff	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Temporary staff	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Seconded National Experts										
TOTAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– The staff requirements take into account that the four components and the CRRS constitute a portfolio of projects with dependencies (i.e. a programme). To manage the dependencies between projects, a programme management team is created comprising the programme and project managers and the profiles (often referred to as architects) that need to define the common elements between them. The programme/project realisation also requires profiles for programme and project support.

– The staff requirements per project have been estimated by analogy with previous projects (Visa Information System) and distinguishing the project completion phase and the operational phase.

– The profiles that need to stay on during the operations phase are recruited as temporary agents. The profiles required during programme/project execution are recruited as contract agents. To ensure the expected continuity of tasks and for keeping knowledge within the Agency, the number of posts is spread almost 50/50 over temporary agents and contract agents.

– The assumption is made that there would be no additional staff required to undertake the ECRIS-TCN high availability project and that eu-LISA project staffing is done re-using existing staff from projects that come to completion in that period of time.

These estimates are based on the following staffing levels:

For contract staff:

3.2.1. outputs EU-LISA (is equal to T1) in number of persons	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (formula)
Contract Staff										-
Programme/project mgt	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Programme/project office	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Quality Assurance	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Financial and Procurement	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Financial mgt										*0,0*
Budgetary planning and control										*0,0*
Procurement/contract mgt	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Technical experts	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Testing	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
System monitoring	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Common (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
General Coordination	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Human resources	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Sub- total Contract Staff	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

For Temporary Agents:

Temporary staff										
Programme/project mgt	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programme mgr	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Project mgt	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Programme/project office	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
Shared BMS	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Financial and Procurement	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Financial mgt	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Budgetary planning and control	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Procurement/contract mgt	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Technical experts	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Security	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architects	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Testing	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
Shared BMS	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
System monitoring	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Training	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Training	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Human resources	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Other	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Data protection specialist	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Sub-total Temporary Agents	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Estimated impact on appropriations of an administrative nature

3.2.4.1. DG Home: 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
HEADING 5 of the multiannual financial framework										
Human resources DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Other administrative expenditure	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotal HEADING 5 of the multiannual financial framework	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Outside HEADING 5[97] of the multiannual financial framework	(not used)									
Human resources										
Other expenditure of an administrative nature										
Subtotal outside HEADING 5 of the multiannual financial framework										

TOTAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[97] 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.

3.2.4.2. Estimated requirements of human resources

– ☐ 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 **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
• Establishment plan posts (officials and temporary staff)										
18 01 01 01 (Headquarters and Commission's Representation Offices) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (Delegations)										
XX 01 05 01 (Indirect research)										
10 01 05 01 (Direct research)										
• External staff (in Full Time Equivalent unit: FTE)[98]										
XX 01 02 02 (AC, AL, END, INT and JED in the delegations)										
XX 01 04 **yy** 99 - at Headquarters										
XX 01 04 **yy** 99 - in Delegations										
XX 01 05 02 (AC, END, INT - Indirect research)										
10 01 05 02 (AC, END, INT - Direct research)										
Other budget lines (specify)										
TOTAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 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::

Project monitoring and follow-up. 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. As the programme is an additional activity compared with existing workloads, additional staff are required. This staff increase is limited in terms of duration and covers only the development period.

Management of UMF

The Commission will manage the UMF standard on a day-to-day basis. Two officials are required for this purpose: one person as law enforcement expert and another person with sound knowledge of business modelling as well as ICT knowledge.

The Universal Message Format (UMF) establishes a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. UMF defines a common vocabulary and logical structures for commonly exchanged information with the objective to

98 AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JED= Junior Experts in Delegations.

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

facilitate interoperability by enabling the creation and reading of the contents of the exchange in a consistent and semantically equivalent manner.

In order to ensure uniform conditions for the implementation of the Universal Message Format, implementing powers are proposed to be conferred on the Commission. Those powers are proposed to be exercised in accordance with 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

3.2.5. Compatibility with the current multiannual financial framework

– ☐ The proposal/initiative is compatible the current multiannual financial framework.

– ☒ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. The ISF Borders Regulation is the financial instrument where the budget for the implementation of the interoperability initiative has been included. It provides in Article 5(b) that EUR 791 million is to be implemented through a programme for developing IT systems based on existing and/or new IT systems, supporting the management of migration flows across the external borders subject to the adoption of the relevant Union legislative acts and under the conditions laid down in Article 15. Of this EUR 791 million, EUR 480.2 million is reserved for the development of the EES, EUR 210 million for ETIAS and EUR 67.9 million for the revision of SIS II. The remainder (EUR 32.9 million) is to be reallocated using ISF-B mechanisms. **The current proposal requires EUR 32.1 million for the current MFF period which fits with the remaining budget**.

The conclusion in the box above on the amount required of EUR 32.1 million is the result of the following computation sheet:

COMMITMENTS										
3.2. Estimated impact on expenditure DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horiz)**
18 02 01 03 - Smart Borders (covers the support to MS)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Total (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formula)**
T1: Staff expenditures	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Infrastructure and Operating Expenditure	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Operational Expenditure	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Infrastructure and Operating Expenditure	0	0	0	0	0	0	0	0	0	0
T3: Operational Expenditure	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Infrastructure and Operating Expenditure	0	0	0	0	0	0	0	0	0	0
T3: Operational Expenditure	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex - EBCG										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Infrastructure and Operating Expenditure	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Operational Expenditure	0	0	0	0,183	2,200	0	0	0	0	2,383
Total (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Heading 5 'Administrative expenditure'										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework.

3.2.6. Third-party contributions

– The proposal/initiative **does not** provide for co-financing by third parties.

3.3. Estimated impact on revenue

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

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

– ☐ on own resources

– ☒ on miscellaneous revenue

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[100]								
		Year **2019**	Year **2020**	Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
Article 6313 - Contribution Schengen associated countries (CH, NO, LI, IS)…… …….		pm	pm	pm	pm	pm	pm	pm	pm	pm

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

18.0207

Specify the method for calculating the impact on revenue.

The budget shall include a contribution from countries associated with the implementation, application and development of the Schengen acquis and the Eurodac related measures as laid down in the respective agreements.

[100] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25 % for collection costs.