EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 791 final

2020/0350 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Crime and terrorism operate across borders, as criminals and terrorists exploit the advantages brought about by globalisation and mobility. Consequently, the information that third countries share with the EU on criminal and terrorist activity is increasingly relevant for EU internal security, at the EU external border as well as within the territory of the Union. However, there are currently limits in the sharing of third-country sourced information on persons who have been suspected or convicted of criminal and terrorist offences within the EU.[1] More specifically, there are **limits in the sharing of third-country sourced information with frontline officers in the Member States** (police officers and border guards) when and where they need it. The same applies to information shared by international organisations with Europol.

For example, this **problem arises in the context of on-going efforts to detect foreign terrorist fighters**. Europol's Terrorism Situation and Trend report[2] of June 2020 states that while many foreign terrorist fighters are believed to have been either killed or confined in detention or refugee camps in north-eastern Syria, there are a substantial number of foreign terrorist fighters still unaccounted for. According to the report, chaos and lack of information from the conflict zone have resulted in the information available to Member States about foreign terrorist fighters being limited and unverifiable. Likewise, the June 2020 Council Conclusions on EU external action on preventing and countering terrorism and violent extremism recognise that *"foreign terrorist fighters will remain a major common security challenge for the years to come"*, calling for enhanced and timely cooperation and information sharing among Member States, with Europol and other relevant EU actors.[3] However, the information that Europol puts into its information systems, notably the result of its own analysis of third-country sourced data, does not reach end-users in the same way as information that Member States provide to the Schengen Information System (SIS).

Europol estimates that currently **information on approximately 1000 non-EU foreign terrorist fighters**, provided by trusted third countries to Europol and individual Member States, **has not been inserted into SIS**. As the most widely used information-sharing database in the EU, SIS provides frontline officers real-time with direct access to alerts on persons and objects, including alerts on suspects and criminals. In the absence of alerts in SIS on the 1000 non-EU foreign terrorist fighters, there is a risk that border guards do not detect them when they seek to enter the EU, or when police officers check them within the territory of the EU. This constitutes a considerable security gap.

---

1 In this context, the reference to '*suspects and criminals*' covers: (a) Persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence. (b) Persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020.

3 https://www.consilium.europa.eu/en/press/press-releases/2020/06/16/preventing-and-countering-terrorism-and-violent-extremism-council-adopts-conclusions-on-eu-external-action/.

In that respect, the June 2018 Council Conclusions on strengthening the cooperation and use of SIS to deal with persons involved in terrorism or terrorism-related activities already recalled the need to "*ensure that information on FTFs is consistently and systematically uploaded to European systems and platforms*".[4] The Council referred to a "*three-tier information sharing approach regarding FTFs by making optimal and consistent use of SIS and Europol data that Europol processes for cross-checking and for analysis in the relevant Analysis projects.*" However, **Member States are not always able to enter information from third countries or international organisations on foreign terrorist fighters in SIS** to make it available to the frontline officers in other Member States. First, some third countries share data on suspects and criminals only with Europol and possibly with some Member States. Second, even if a Member State receives the information on suspects and criminals directly from the third country or via Europol, it might not be able to issue an alert on the person concerned due to restrictions in national law (e.g. the need to establish a link to national jurisdiction). Third, the Member State may not have the means to sufficiently analyse and verify the received information. This leads to a gap between the information on suspects and criminals that third countries make available to Europol and Member States, and the availability of such information to frontline officers when and where they need it.

In terms of a **possible EU-level solution**, it is widely acknowledged that **Europol** holds valuable information on suspects and criminals that it received from third countries and international organisations. Once Europol analysed information it received from third countries and international organisations on suspects and criminals, including by cross checking it against information it already holds in its databases to confirm the accuracy of the information and complement it with other data, Europol needs to make the result of its analysis available to all Member States. To that end, Europol uses its information systems to make an analysis of third-country sourced information on suspects and criminals available to Member States. Europol will also enter third-country sourced information into the watchlist of the European Travel Information and Authorisation System (ETIAS) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the EU external borders.[5] The watchlist will support Member States in assessing whether a person applying for a travel authorisation poses a security risk.

However, **Europol is not able to provide directly and in real time frontline officers in the Member States with the third-country sourced information it holds on suspects and criminals**. Frontline officers do not have immediate access to Europol's information systems or to the data entered by Europol in the ETIAS watchlist. Europol's information systems support the work of investigators, criminal intelligence officers and analysts in the Member States. While it is for each Member State to decide which competent national authorities are allowed to cooperate directly with Europol[6], there is typically no possibility for frontline officers to access Europol's information systems.

While Europol is able to check persons in SIS, and from March 2021 will be informed about hits on terrorism-related alerts issued by other Member States, Europol is not able to issue alerts in SIS as the most widely used information-sharing database in the EU that is directly accessible for border guards and police officers. Crucial third-country sourced information held by Europol on suspects and criminals might therefore not reach the end-users at national level when and where they need it. This includes Europol's analysis of data it received from

4 https://www.consilium.europa.eu/media/36284/st09680-en18.pdf.
5 Regulation (EU) 2018/1240.
6 Article 7(5) of Regulation (EU) 2016/794.

third countries and international organisations on foreign terrorist fighters, but also on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse).

Reflecting the differences in purpose between Europol's information systems and SIS, there is a major difference in the outreach of these systems.

	Europol Information System	**Schengen Information System**
Users	8 587 users (end of 2019)	Every frontline officer in the Member States[7] (border guards and police officers)
Number of checks (in 2019)[8]	5.4 million	6.6 billion

In order to address this security gap, **the objective of this proposal is to establish a new alert category specifically for Europol**, in order to provide information directly and in real-time to front-line officers. To this end, it is necessary for both Regulation (EU) 2016/794 European Union Agency for Law Enforcement Cooperation (Europol)[9] and Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters to be amended.[10] Due to variable geometry, whereas different Member States participate in these two Regulations, the amendments are presented in two separate, but logically linked proposals.

The present proposal concerns the amendment of Regulation (EU) 2018/1862. The proposal is intended to enable **Europol to issue 'information alerts'** on suspects and criminals as a new alert category in SIS, for exclusive use by Europol in specific and well-defined cases and circumstances. This is an important paradigm change for SIS, as until now, only Member States could enter, update and delete data in SIS and Europol had 'read-only' access covering all alert categories. Europol would be able to issue alerts on the basis of **its analysis of third-country sourced information or information from international organisations**, within the

[7] 25 Member States participate in the Schengen Information System (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden). Ireland and Cyprus are in the process of being connected to the system in 2021. Four Schengen Associated Countries are connected to the system (Iceland, Liechtenstein, Norway and Switzerland). Europol, teams deployed by the EBCGA and the EU Agency for criminal justice cooperation Eurojust have access to specific parts of the system but cannot issue alerts in the system.

[8] For the Schengen Information System, the table shows all checks carried out in 2019 by all users who have access to the system. When checking the Schengen Information System, users are checking data against those alerts to which they have access (which does not in all cases include law enforcement alerts).

[9] 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).*

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

scope of crimes falling under Europol's mandate and only on third-country nationals who are not beneficiaries of free movement rights.

The **purpose of the new alert category** is that in case of a 'hit', the alert would inform the frontline officer that the person concerned is suspected of being involved in a criminal offence falling within the competence of Europol. As an action to be taken, the fact that the person was located and the place, time and reason for the check would be reported back to Europol (via the national SIRENE Bureau). Beyond this reporting there would be no further obligation on the Member State where the 'hit' occurred. Nevertheless, the Member State executing the alert would be able to determine, on a case-by-case basis, including based on the background information received from Europol, whether further measures need to be taken with regard to the person under national law and at the full discretion of that Member State.

As the exchange of information from third-countries or international organisations on suspects and criminals includes the processing of personal data, the assessment of policy options to address the identified problem takes **full account of the obligation to respect Fundamental Rights and notably the right to the protection of personal data**.

- **Consistency with existing policy provisions in the policy area and with other Union policies**

This proposal is closely linked with and complements other Union policies, namely:

(1) internal security, in particular the 'Counter-Terrorism package' this proposal forms part of;

(2) data protection, insofar as this proposal ensures the protection of fundamental rights of individuals whose personal data is processed in SIS;

(3) the Union's external policies, notably the work of EU delegations and counter-terrorism/security policy in third countries.

This proposal is also closely linked with and complements existing Union legislation, namely:

(1) on Europol, insofar as this proposal grants Europol additional rights to process and exchange data, within its mandate, in SIS;

(2) on the management of the external borders: the proposal complements the principle in the Schengen Borders Code[11] of conducting systematic checks against relevant databases of all travellers upon entry and exit to the Schengen area, as established in response to the phenomenon of foreign terrorist fighters;

(3) on the European Travel Information and Authorisation System (ETIAS) which provides for a thorough security assessment, including a check in SIS, of third country nationals who intend to travel to the EU;

(4) on the Visa Information System (VIS)[12] including a check in SIS, of third country nationals who apply for a visa.

[11] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

[12] 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. 60–81).

Furthermore, the proposal includes additional amendments to Regulation (EU) 2018/1862 in order to align its provisions concerning data protection, in particular the right of access, rectification of inaccurate data and erasure of unlawfully stored data, remedies and liability with Regulation (EU) 2016/794 and Regulation (EU) 2018/1725 insofar as those alignments are necessary due to the new alert category to be entered by Europol.

Finally, as a consequence of this proposal, Union legislation on both ETIAS and the VIS will need to be assessed to determine whether to include, as part of the advance security assessment, the new SIS alert category within the automated processing carried out by ETIAS and VIS. It is not possible to carry out this assessment at this stage, as the regulations on ETIAS and VIS are currently under negotiation in the European Parliament and Council. The Commission will present consequential amendments for each of these instruments after the negotiations have been concluded.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

This proposal amends Regulation (EU) 2018/1862 and uses one of its legal bases, namely Article 88(2)(a) of the Treaty on the Functioning of the European Union (TFEU) as the legal basis. Article 88 of the TFEU refers to the mandate of Europol and point (2)(a) of this Article specifically to the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies.

• Variable geometry

This proposal builds upon the provisions of the Schengen acquis related to police cooperation and judicial cooperation in criminal matters. Therefore, the following consequences in relation to the various protocols and agreements with associated countries have to be considered:

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

Ireland: Ireland is taking part in this Regulation in accordance with Article 5(1) of Protocol No 19 annexed to the TEU and to the TFEU and Article 6(2) of Council Decision 2002/192/EC[13] and Council Implementing Decision (EU) 2020/1745[14].

Iceland and Norway: this Regulation will constitute a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen

[13] Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

[14] Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of certain provisions of the Schengen acquis in Ireland (OJ L 393, 23.11.2020, p. 3).

acquis[15], which fall within the area referred to in Article 1, point (G) of Council Decision 1999/437/EC[16].

Switzerland: this Regulation will constitute a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[17], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA[18].

Liechtenstein: this Regulation will constitute a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[19], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[20].

Bulgaria and Romania: this Regulation will constitute an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2005 Act of Accession and should be read in conjunction with Council Decisions 2010/365/EU[21] and (EU) 2018/934[22].

Croatia: this Regulation will constitute an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2011 Act of Accession and should be read in conjunction with Council Decision (EU) 2017/733[23].

---

15 OJ L 176, 10.7.1999, p. 36.

16 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

17 OJ L 53, 27.2.2008, p. 52.

18 Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

19 OJ L 160, 18.6.2011, p. 21.

20 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

21 Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Bulgaria and Romania (OJ L 166, 1.7.2010, p. 17).

22 Council Decision (EU) 2018/934 of 25 June 2018 on the putting into effect of the remaining provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Bulgaria and Romania (OJ L 165, 2.7.2018, p. 37).

23 Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Croatia (OJ L 108, 26.4.2017, p. 31).

- **Subsidiarity (for non-exclusive competence)**

According to the principle of subsidiarity laid down in Article 5(3) TEU, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

This proposal will develop and build upon the existing SIS, which has been operational since 1995. The original intergovernmental framework was replaced by Union instruments on 9 April 2013 [Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA]. On 28 November 2018, three new Regulations were adopted on SIS: Regulation (EU) 2018/1860[24] on the use of SIS in the field of return, Regulation (EU) 2018/1861[25] on the use of SIS in the field of borders and Regulation (EU) 2018/1862 on the use of SIS in the field of police cooperation and judicial cooperation in criminal matters. These Regulations will repeal and replace the previous legal framework governing SIS at the end of 2021.

A full subsidiarity analysis has been carried out on previous occasions; this initiative is focused on introducing a new alert category to be entered in SIS by Europol, by amending Regulation (EU) 2018/1862.

The considerable level of information exchange between Member States and Europol through SIS cannot be achieved via decentralised solutions. By reason of the scale, effects and impacts of the action, this proposal can be better achieved at Union level. The objectives of this proposal encompasses, inter alia, the procedural and legal requirements for Europol to enter alerts in SIS as well as technical requirements for Europol to establish a technical interface through which it can enter, update and delete alerts.

If existing limitations to SIS are not addressed, there is a risk that numerous opportunities for maximised efficiency and EU added value are missed and that there are blind spots concerning security threats impeding the work of competent authorities.

- **Proportionality**

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

The proposed initiative constitutes an amendment of SIS in relation to police cooperation and judicial cooperation in criminal matters. In terms of the right to protection of personal data, this proposal complies with the proportionality principle as it provides for specific procedures and safeguards when entering alerts by Europol as well as specific alert deletion rules and does not require the collection and storage of data for longer than is absolutely necessary to allow the system to function and meet its objectives. SIS alerts entered by Europol will contain only the data which is required to identify a person. All other additional details are provided via the SIRENE Bureaux enabling the exchange of supplementary information. In addition, the proposal provides for the implementation of all necessary safeguards and mechanisms required for the effective protection of the fundamental rights of the data subjects, particularly the protection of their private life and personal data.

The envisaged measure is proportionate in that it does not go beyond what is necessary in terms of action at EU level to meet the defined objectives. The alert entered by Europol will

[24] OJ L 312, 7.12.2018, p. 1.
[25] OJ L 312, 7.12.2018, p. 14.

be a ‘last resort’ solution in cases when Member States are not able to or do not intend to enter alerts on the person concerned, to which recourse is possible only in cases when entering the alert is necessary and proportionate. The action to be taken will be limited to providing information on the place and time of the check in which the hit on the Europol alert occurred.

- **Choice of the instrument**

The proposed revision will take the form of a Regulation and will amend Regulation (EU) 2018/1862 in order to introduce a new alert category to be entered in SIS by Europol. The legal base of this proposal is point (a) of Article 88(2) the TFEU which is also the legal basis of Regulation (EU) 2018/1862 that it will amend.

The form of a Regulation of the European Parliament and of the Council has to be chosen because the provisions are to be binding and directly applicable in all Member States as well as by Europol. The proposal will build on an existing centralised system through which Member States cooperate, something which requires a common architecture and binding operating rules.

The legal basis requires the use of the ordinary legislative procedure.

Furthermore, the proposal provides for directly applicable rules enabling data subjects' access to their own data and remedies without requiring further implementing measures in this respect. As a consequence, only a Regulation can be chosen as a legal instrument.

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

- **Stakeholder consultations**

To ensure that the general public interest is properly considered in the Commission's approach to strengthening Europol’s mandate, including the task to enter alerts in SIS, the Commission services identified relevant stakeholders and consulted them throughout the preparation of this initiative. The Commission services sought views from a wide range of subject matter experts, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to enhancing Europol’s capabilities in supporting Member States to effectively prevent and investigate crime.

During the consultation process, the Commission services applied a variety of methods and forms of consultation.[26] They included:

- the consultation on the Inception Impact Assessment, which sought views from all interested parties;
- targeted stakeholder consultation by way of a questionnaire;
- expert interviews; and
- targeted thematic stakeholder workshops that focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and

[26] It should be noted that consultation activities used served to collect information and arguments. They are not surveys, as they refer to non-representative samples of the stakeholders or the general population and thus do not allow for conclusions.

specificities of the subject, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

The diversity of perspectives proved valuable in supporting the Commission to ensure that its initiative addresses the needs, and took account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary and indispensable data, facts and views on the relevance, effectiveness, efficiency, coherence and EU added value of this initiative.

Taking into consideration the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

Stakeholders are generally supportive of strengthening Europol's legal mandate to support Member States in preventing and combatting serious crime and terrorism.

The results of the consultation activities were incorporated throughout the impact assessment and the preparation of the initiative.

- **Impact assessment**

In line with Better Regulation requirements, an Impact Assessment has been prepared accompanying the proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation (Europol) amending Regulation (EU) No 2016/794. This report has assessed the issue of introducing a new alert category in SIS exclusively for Europol, reflecting Europol's role and competences, as well as the necessary safeguards.

Several legislative policy options have been considered. The following policy options have been assessed in full detail:

- Policy option 1: enabling Europol to issue 'discreet check' alerts in SIS;
- Policy option 2: introducing a new alert category in SIS to be used exclusively by Europol.

Following a detailed assessment of the impact of these policy options, it was concluded that the preferred policy option is option 2. This preferred policy option is reflected in this initiative.

The preferred policy option 2 responds effectively to the identified problems and would enhance Europol's capability to provide frontline officers with its analysis of third-country sourced information on suspects and criminals.

- **Fundamental rights**

This proposal adds a new alert category – to be entered by Europol – to an existing system, and hence builds upon important and effective safeguards that have already been put in place. Nevertheless, as the system will process data for a new purpose, there are potential impacts on an individual's fundamental rights. These have been thoroughly considered, and additional safeguards have been put in place to limit the processing of data by Europol to what is strictly necessary and operationally required.

Clear data review timeframes have been set out in this proposal for the new alert category. The review period is set at maximum one year, which is the shortest review period applied in

SIS. There is explicit recognition of and provision for individuals' rights to access and rectify data relating to them, and to request deletion in line with their fundamental rights.

The development and continued effectiveness of SIS will contribute to the security of persons within society.

The proposal guarantees the data subject's right to effective remedies available to challenge any decisions, which shall in any case include an effective remedy before a court or tribunal in line with Article 47 of the Charter of Fundamental Rights.

4. BUDGETARY IMPLICATIONS

The present proposal widens the scope of application of the current SIS by introducing a new alert category for Europol.

The financial statement attached to this proposal reflects the changes required for establishing this new alert category in Central SIS by eu-LISA, the EU Agency responsible for the management and development of Central SIS. On the basis of an assessment of the various aspects of the work required in relation to the Central SIS by eu-LISA the proposed Regulation will require a global amount of EUR 1,820,000 for the period 2021-2022.

The proposal will also have an impact on the Member States requiring them to update their national systems, connected to Central SIS, to be able to display the Europol alert to their end-users. The expenses related to the development of the national systems connected to Central SIS are to be covered by the resources available to the Member States under the new Multiannual Financial Framework 2021-2027 for the development and maintenance of SIS.

The proposal will also require Europol to set up a technical interface for entering, updating and deleting data in Central SIS. The financial statement attached to the proposal to amend the Europol regulation covers the expenses related to the set-up of this interface by Europol.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

On the basis of Regulation (EU) 2018/1862, the Commission, Member States and eu-LISA will regularly review and monitor the use of SIS, to ensure that it continues to function effectively and efficiently.

The Commission will be assisted by the SIS-SIRENE Committee (Police formation) to implement technical and operational measures as described in the proposal by amending the relevant Commission Implementing Decisions.

Article 51 of Regulation (EU) 2018/1862 foresees the evaluation of the use of SIS by Europol, Eurojust and the European Border and Coast Guard Agency carried out by the Commission at least every five years. This evaluation will cover the procedures of Europol to enter data in SIS. Europol will have to ensure adequate follow-up to the findings and recommendations stemming from the evaluation. A report on the results of the evaluation and follow-up to it will be sent to the European Parliament and to the Council.

In addition, Regulation (EU) 2018/1862 includes provisions in Article 74(9) for a formal, regular review and evaluation process that will be also applicable to the new alert category introduced by this amendment.

Every four years, the Commission is required to conduct, and share with the Parliament and the Council, an overall evaluation of SIS and the exchange of information between Member States. This will:

- examine results achieved against objectives;
- assess whether the underlying rationale for the system remains valid;
- examine how the Regulation is being applied to the central system;
- evaluate the security of the central system;
- explore implications for the future functioning of the system.

Every two years, eu-LISA is required to report to the European Parliament and the Council on the technical functioning – including security – of SIS, the communication infrastructure supporting it, and the bilateral and multilateral exchange of supplementary information between Member States as well as the Automated Fingerprint Identification System.

eu-LISA is also charged with providing daily, monthly and annual statistics on the use of SIS, ensuring continuous monitoring of the system and its functioning against objectives.

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

The proposal enables Europol to issue 'information alerts' on suspects and criminals as a new alert category in SIS, for exclusive use by Europol in specific and well-defined cases and circumstances. Europol would be able to issue such alerts on the basis of its analysis of third-country sourced information or information from international organisations, and within the scope of crimes falling under Europol's competence and only on third-country nationals.[27] This specific objective limits in the sharing of third-country sourced information to suspects and criminals.

The purpose of the new alert category is that in case of a 'hit', the alert would inform the frontline officer that Europol holds information on the person. More specifically, the alert would inform that Europol holds information giving grounds to consider that the person is intending to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future.

The proposal sets out detailed provisions on the procedural requirements that Europol is required to fulfil prior to entering an alert in SIS. These procedural steps ensure the legality of entering the alert as well as the priority of alerts entered by Member States and that any objection by Member States is taken into account.

First, Europol is to analyse the information received by third countries or international organisations, e.g. by way of checking it against other available information, to verify its accuracy and to complement the information picture. If necessary, Europol has to carry out further information exchange with the third country or international organisation. Europol also has to assess whether entering the alert is necessary for achieving its objectives as laid down in Regulation (EU) 2016/794.

[27] In line with Article 36 of Regulation (EU) 2018/1862, this would cover persons where there is a clear indication that they intend to commit or are committing any of the crimes for which Europol is competent, or persons where an overall assessment (in particular on the basis of past criminal offences) gives reasons to believe that they may commit in future one of the crimes for which Europol is competent.

Second, Europol has to check that there is no existing alert in SIS on the same person.

Third, Europol has to share the information collected on the person concerned with all Member States and carry out a prior consultation in order to confirm that no Member State intends to enter the alert themselves based on the information collected by Europol and that Member States do not object to the alert being entered by Europol. These provisions ensure that if a Member State considers that they have sufficient information and grounds to fulfil the requirements of Regulation (EU) 2018/1862 as well as their national provisions for entering the alert themselves, then they have the possibility to do so and this alert takes precedence. In this case, Member States have the possibility to determine the relevant alert category available to them, based on Regulation (EU) 2018/1862 and issue an alert. Member States also have the possibility to object to the alert being entered by Europol, in justified cases, in particular, if their national security so requires or when it is likely that the alert would represent a risk for official or legal inquiries, investigations or procedures or if they obtain new information about the person who is the subject of the alert which changes the assessment of the case.

In order to ensure data protection monitoring by the European Data protection Supervisor, Europol shall keep detailed records relating to the entry of the alert in SIS and the grounds for such entry that permit verification of compliance with the substantive and procedural requirements.

Finally, Europol has to inform all Member States of the entry of the alert in SIS through the exchange of supplementary information.

In addition, the proposals aligns the obligations and requirements of Europol when entering alerts in SIS with alert issuing Member States. These requirements concern: categories of data, proportionality, minimum data content for an alert to be entered, entering biometric data, general data processing rules, quality of the data in SIS as well as rules on distinguishing between persons with similar characteristics, misused identity and links.

As an action to be taken, the frontline officer would be required to report immediately the occurrence of the 'hit' to the national SIRENE Bureau, which would in turn contact Europol. The frontline officer would only report that the person who is subject of an alert was located and would indicate the place, time and reason for the check carried out. Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member State where the 'hit' occurred. The 'information alert' would not impose an obligation on Member States' frontline officers to discreetly check the person under alert and collect a set of detailed information if they encounter him/her at the external border or within the territory of the EU. Rather, the Member State executing the alert would be free to determine, on a case-by-case basis, including based on the background information received from Europol, whether further measures need to be taken with regard to the person concerned. Such further measures would take place under national law and subject to the full discretion of the Member State.

Similarly to other alert categories, the proposal defines the review period for alerts entered by Europol as well as the alert deletion rules which are specific to this type of alert. As a general rule, an alert should be kept only for the time that is necessary to achieve the purpose for which it was entered. An alert entered by Europol in SIS should be deleted, in particular, if the person who is the subject of the alert no longer falls under the scope of this alert category, a Member State objects the insertion of such alert, another alert is entered in SIS by a Member State or if Europol becomes aware that the information received from the third country or international organisation was incorrect or was communicated to Europol for unlawful purposes, for example if sharing the information on the person was motivated by political reasons.

The proposal includes amendments to Regulation (EU) 2018/1862 in order to align its provisions concerning data protection, in particular the right of access, rectification of inaccurate data and erasure of unlawfully stored data, remedies and liability with Regulation (EU) 2016/794 and Regulation (EU) 2018/1725 insofar as those alignments are necessary due to the new alert category to be entered by Europol.

2020/0350 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol

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 point (a) of Article 88(2) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Schengen Information System ('SIS') constitutes an essential tool for maintaining a high level of security within the area of freedom, security and justice of the Union by supporting operational cooperation between national competent authorities, in particular border guards, the police, customs authorities, immigration authorities, and authorities responsible for the prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties. Regulation (EU) 2018/1862 of the European Parliament and of the Council[28] constitutes the legal basis for SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of Part Three of the Treaty on Functioning of the European Union (TFEU).

(2) Alerts on persons and objects entered in SIS are in real time made available directly to all end-users of the competent national authorities of Member States that use SIS pursuant to Regulation (EU) 2018/1862. SIS alerts contain information about a particular person or object as well as instructions for the authorities on what to do when the person or object has been found.

(3) The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794 of the European Parliament and of the Council[29], plays an important role in the use of SIS and in the exchange of supplementary information with Member States on SIS alerts. Nevertheless, according

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

[29] 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. 53–114).

to existing rules, alerts in SIS can only be issued by Member States' competent authorities.

(4) Given the increasingly global nature of serious crime and terrorism brought about by growing mobility, the information that third countries and international organisations, such as the International Criminal Police Organization and the International Criminal Court, obtain about criminals and terrorists is increasingly relevant for the Union's security. Such information should contribute to the comprehensive efforts to ensure internal security in the European Union. Some of this information is only shared with Europol. While Europol holds valuable information received from external partners on serious criminals and terrorists, it cannot issue alerts in SIS. Member States are also not always able to issue alerts in SIS on the basis of such information.

(5) In order to bridge the gap in information sharing on serious crime and terrorism, in particular on foreign terrorist fighters – where the monitoring of their movement is crucial – it is necessary to ensure Europol is able to make this information available directly and in real-time to front-line officers in Member States.

(6) Europol should therefore be authorised to enter alerts in SIS pursuant to Regulation (EU) 2018/1862, in full respect of fundamental rights and data protection rules.

(7) To that end, a specific category of alert should be created in SIS, to be issued exclusively by Europol, in order to inform end-users carrying out a search in SIS that the person concerned is suspected of being involved in a criminal offence in respect of which Europol is competent, and in order for Europol to obtain confirmation that the person who is subject to the alert has been located.

(8) In order to assess whether a concrete case is adequate, relevant and important enough to warrant the entry of an alert in SIS, and in order to confirm the reliability of the source of information and the accuracy of the information on the person concerned, Europol should carry out a detailed individual assessment of each case including further consultations with the third country or international organisation that shared the data on the person concerned, as well as further analysis of the case, in particular by cross checking it against information it already holds in its databases, to confirm the accuracy of the information and complement it with other data on the basis of its own databases. The detailed individual assessment should include the analysis of whether there are sufficient grounds for considering that the person has committed or taken part in, or will commit a criminal offence in respect of which Europol is competent.

(9) Europol should only be able to enter an alert in SIS if the person concerned is not already subject to a SIS alert issued by a Member State. A further precondition for the creation of such an alert should be that Member States do not object to the alert being issued in SIS. Therefore, it is necessary to establish rules on the obligations of Europol prior to entering data in SIS, in particular the obligation to consult the Member States in line with Regulation (EU) 2016/794. It should also be possible for Member States to request the deletion of an alert by Europol, in particular if they obtain new information about the person who is the subject of the alert, if their national security requires so or when it is likely that the alert would represent a risk for official or legal inquiries, investigations or procedures.

(10) Europol should keep records of the individual assessment of each case, which should include the grounds for entering the alert, for the purposes of verifying the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.

In accordance with Regulation (EU) 2016/794, Europol should co-operate with the European Data Protection Supervisor and make these records available upon request, so that they can be used for monitoring processing operations.

(11) It is necessary to establish rules concerning the deletion of alerts entered in SIS by Europol. An alert should be kept only for the time required to achieve the purpose for which it was entered. It is therefore appropriate to set out detailed criteria to determine when the alert should be deleted. An alert entered by Europol in SIS should be deleted in particular if a Member State objects, another alert is entered in SIS by a Member State, or if Europol becomes aware that the information received from the third country or international organisation was incorrect or was communicated to Europol for unlawful purposes, for example if sharing the information on the person was motivated by political reasons.

(12) When entering alerts in SIS, Europol should be bound by the same requirements and obligations applicable to the Member States pursuant to Regulation (EU) 2018/1862 when they enter alerts in SIS. In particular, Europol should comply with common standards, protocols and technical procedures established to ensure the compatibility of its technical interface with Central SIS for the prompt and effective transmission of data. Requirements concerning general data processing rules, proportionality, data quality, data security, reporting and obligations related to collecting statistics applicable to Member States when entering alerts in SIS should apply to Europol as well.

(13) Regulation (EU) 2018/1725 of the European Parliament and of the Council[30] and Regulation (EU) 2016/794 should apply to the processing of personal data by Europol when carrying out its responsibilities under this Regulation. The European Data Protection Supervisor should carry out periodic audits on the data processing of Europol concerning SIS and the exchange of supplementary information.

(14) Since the objectives of this Regulation, namely the establishment and regulation of a specific alert category issued by Europol in SIS in order to exchange information on persons who represent a threat to the internal security of the European Union, cannot be sufficiently achieved by the Member States, but can rather, by reason of their nature be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(15) This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation fully respects the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking to ensure a safe environment for all persons residing on the territory of the Union.

(16) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this

[30] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(17) Ireland is taking part in this Regulation in accordance with Article 5(1) of Protocol No 19 annexed to the TEU and to the TFEU and Article 6(2) of Council Decision 2002/192/EC[31] and Council Implementing Decision (EU) 2020/1745[32].

(18) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis*[33], which fall within the area referred to in Article 1, point (G) of Council Decision 1999/437/EC[34].

(19) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[35], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA[36].

(20) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[37], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[38].

---

31 Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

32 Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of certain provisions of the Schengen acquis in Ireland (OJ L 393, 23.11.2020, p. 3).

33 OJ L 176, 10.7.1999, p. 36.

34 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

35 OJ L 53, 27.2.2008, p. 52.

36 Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

37 OJ L 160, 18.6.2011, p. 21.

38 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen

(21) As regards Bulgaria and Romania, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2005 Act of Accession and should be read in conjunction with Council Decisions 2010/365/EU[39] and (EU) 2018/934[40].

(22) As regards Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2011 Act of Accession and should be read in conjunction with Council Decision (EU) 2017/733[41].

(23) Concerning Cyprus, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 3(2) of the 2003 Act of Accession [to add eventual Council Decision].

(24) The European Data Protection Supervisor was consulted, in accordance with Article 41(2) of Regulation (EU) 2018/1725 of the European Parliament and the Council[42].

(25) Regulation (EU) No 2018/1862 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1
Amendments to Regulation (EU) 2018/1862

(1) In Article 2, paragraph 2 is replaced by the following:

'2. This Regulation also lays down provisions on the technical architecture of SIS, on the responsibilities of the Member States, the European Union Agency for Law Enforcement Cooperation ('Europol') and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), on data processing, on the rights of the persons concerned and on liability.'

(2) In Article 3, the following point is added:

'(22) 'third-country national' means any person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, with the exception of persons who are beneficiaries of the right of free movement within the Union in accordance with Directive 2004/38/EC or with an agreement between the Union or the Union and its Members States on the one hand, and a third country on the other hand;'

(3) Article 24 is amended as follows:

---

acquis, relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

39 Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Bulgaria and Romania (OJ L 166, 1.7.2010, p. 17).

40 Council Decision (EU) 2018/934 of 25 June 2018 on the putting into effect of the remaining provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Bulgaria and Romania (OJ L 165, 2.7.2018, p. 37).

41 Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Croatia (OJ L 108, 26.4.2017, p. 31).

42 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(a) paragraph 1 is replaced by the following:

‘1. Where a Member State considers that to give effect to an alert entered in accordance with Article 26, 32, 36 or 37a is incompatible with its national law, its international obligations or essential national interests, it may require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. Flags on alerts entered in accordance with Article 26, 32 or 36 shall be added by the SIRENE Bureau of the issuing Member State, flags on alerts entered in accordance with Article 37a shall be added by Europol.’

(b) paragraph 3 is replaced by the following:

‘3. If in particularly urgent and serious cases, an issuing Member State or Europol requests the execution of the action, the executing Member State shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.’

(4) The following Chapter IXa is inserted:

‘CHAPTER IXa

ALERTS ENTERED BY EUROPOL ON PERSONS OF INTEREST

Article 37a
Objectives and conditions for entering alerts

1. Europol may enter alerts on persons in SIS for the purpose of informing end-users carrying out a search in SIS of the suspected involvement of those persons in a criminal offence in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794, as well as for the purpose of obtaining information in accordance with Article 37b of this Regulation that the person concerned has been located.

2. Europol may only enter an alert in SIS on persons who are third-country nationals on the basis of information received from a third country or an international organisation in accordance with Article 17(1)(b) of Regulation (EU) 2016/794, where the information relates to one of the following:

(a) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794, or who have been convicted of such an offence;

(b) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794.

3. Europol may only enter an alert in SIS after it has ensured all of the following:

(a) an analysis of the data provided in accordance with paragraph 2 confirmed the reliability of the source of information and the accuracy of the information on the person concerned, permitting Europol to determine that that person falls within the scope of paragraph 2, where necessary, after having carried out further exchanges of information with the data provider in accordance with Article 25 of Regulation (EU) 2016/794;

(b) a verification confirmed that entering the alert is necessary for achieving Europol’s objectives as laid down in Article 3 of Regulation (EU) 2016/794;

(c) a search in SIS, carried out in accordance with Article 48 of this Regulation, did not disclose the existence of an alert on the person concerned;

(d) a consultation, involving the sharing of information on the person concerned with Member States participating in Regulation (EU) 2016/794 in accordance with Article 7 of that Regulation, confirmed that:

(i) no intention was expressed by a Member State to enter an alert in SIS on the person concerned;

(ii) no reasoned objection was expressed by a Member State regarding the proposed entry of an alert in SIS on the person concerned by Europol.

4. Europol shall keep detailed records relating to the entry of the alert in SIS and the grounds for such entry to permit verification of compliance with the substantive and procedural requirements laid down in paragraphs 1, 2 and 3. Such records shall be available for the European Data Protection Supervisor on request.

5. Europol shall inform all Member States of the entry of the alert in SIS through the exchange of supplementary information in accordance with Article 8 of this Regulation.

6. The requirements and obligations applicable to the issuing Member State in Articles 20, 21, 22, 42, 56, 59, 61, 62 and 63 shall apply to Europol when processing data in SIS.

Article 37b
Execution of the action based on an alert

1. In the event of a hit on an alert entered by Europol, the executing Member State shall:

(a) collect and communicate the following information:

(i) the fact that the person who is the subject of an alert has been located;

(ii) the place, time and reason for the check;

(b) in accordance with national law, decide whether it is necessary to take any further measures.

2. The executing Member State shall communicate the information referred to in paragraph 1(a) to Europol through the exchange of supplementary information.'

(5) Article 48 is amended as follows:

(a) the title is replaced with the following:

'Entry and processing of data in SIS by Europol'

(b) paragraph 1 is replaced by the following:

'1. Europol shall, where necessary to fulfil its mandate, have the right to access and search data in SIS and to enter, update and delete alerts pursuant to Article 37a of this Regulation. Europol shall enter, update, delete and search SIS data through a dedicated technical interface. The technical interface shall be set up and maintained by Europol in compliance with the common standards, protocols and technical procedures defined in Article 9 of this Regulation and shall allow direct connection to Central SIS.

Europol shall exchange supplementary information in accordance with the provisions of the SIRENE Manual. To that end, Europol shall ensure availability to supplementary information related to its own alerts 24 hours a day, 7 days a week.'

(c) paragraph 4 is replaced by the following:

‘4. Europol's use of information obtained from a search in SIS or from the processing of supplementary information shall be subject to the consent of the Member State that provided the information either as issuing Member State or as executing Member State. If the Member State allows the use of such information, its handling by Europol shall be governed by Regulation (EU) 2016/794. Europol shall only communicate such information to third countries and third bodies with the consent of the Member State that provided the information and in full compliance with Union law on data protection.’

(d) the following paragraph 7a is inserted:

‘7a. The European Data Protection Supervisor shall carry out an audit of the data processing operations of Europol under this Regulation in accordance with international auditing standards at least every four years.’

(6) Article 53 is amended as follows:

(a) the following paragraph 5a is inserted:

‘5a. Europol may enter an alert on a person for the purposes of Article 37a (1) for a period of one year. Europol shall review the need to retain the alert within that period. Europol shall, where appropriate, set shorter review periods.’

(b) paragraphs 6, 7 and 8 are replaced by the following:

‘6. Within the review period referred to in paragraphs 2, 3, 4, 5 and 5a, the issuing Member State, and in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, may, following a comprehensive individual assessment, which shall be recorded, decide to retain the alert on a person for longer than the review period, where this proves necessary and proportionate for the purposes for which the alert was entered. In such cases paragraph 2, 3, 4, 5 or 5a of this Article shall also apply to the extension. Any such extension shall be communicated to CS-SIS.’

‘7. Alerts on persons shall be deleted automatically after the review period referred to in paragraphs 2, 3, 4, 5 and 5a has expired, except where the issuing Member State or in the case of alerts entered in SIS pursuant to Article 37a of this Regulation Europol, has informed CS-SIS of an extension pursuant to paragraph 6 of this Article. CS-SIS shall automatically inform the issuing Member State or Europol of the scheduled deletion of data four months in advance.’

‘8. Member States and Europol shall keep statistics on the number of alerts on persons the retention periods of which have been extended in accordance with paragraph 6 of this Article and transmit them, upon request, to the supervisory authorities referred to in Article 69.’

(7) In Article 55, the following paragraph 6a is inserted:

‘6a. Alerts on persons entered by Europol pursuant to Article 37a shall be deleted upon:

(a) the expiry of the alert in accordance with Article 53;

(b) a decision to delete them by Europol, in particular when after entering the alert Europol becomes aware that the information received under Article 37a (2) was incorrect or was communicated to Europol for unlawful purposes, or when Europol becomes aware or is informed by a Member State, that the person who is the subject of the alert no longer falls under the scope of Article 37a(2);

(c) a notification, through the exchange of supplementary information, of Europol by a Member State, that it is about to enter, or has entered an alert on the person who is the subject of the alert issued by Europol;

(d) a notification of Europol by a Member State participating in Regulation (EU) 2016/794 in accordance with Article 7 of that Regulation, of its reasoned objection to the alert.'

(8) Article 56 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. The Member States shall only process the data referred to in Article 20 for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, 37a, 38 and 40.'

(b) paragraph 5 is replaced by the following:

'5. With regard to the alerts laid down in Articles 26, 32, 34, 36, 37a, 38 and 40 of this Regulation, any processing of information in SIS for purposes other than those for which it was entered into SIS has to be linked with a specific case and justified by the need to prevent an imminent and serious threat to public policy and to public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the issuing Member State or from Europol if the data was entered pursuant to Article 37a of this Regulation, shall be obtained for this purpose.'

(9) In Article 61, paragraphs 1 and 2 are replaced by the following:

'1. Where upon a new alert being entered it becomes apparent that there is already an alert in SIS on a person with the same description of identity, the SIRENE Bureau shall contact the issuing Member State or if the alert was entered pursuant to Article 37a of this Regulation Europol, through the exchange of supplementary information within 12 hours to cross-check whether the subjects of the two alerts are the same person.'

'2. Where the cross-check reveals that the subject of the new alert and the person subject to the alert already entered in SIS are indeed one and the same person, the SIRENE Bureau of the issuing Member State shall apply the procedure for entering multiple alerts referred to in Article 23. By way of derogation, Europol shall delete the alert it has entered as referred to in point (c) of Article 55(6a).'

(10) Article 67 is replaced by the following:

'Article 67

Right of access, rectification of inaccurate data and erasure of unlawfully stored data

(1) Data subjects shall be able to exercise the rights laid down in Articles 15, 16 and 17 of Regulation (EU) 2016/679, in the national provisions transposing Article 14 and Article 16 (1) and (2) of Directive (EU) 2016/680 and in Chapter IX of Regulation (EU) 2018/1725.

(2) A Member State other than the issuing Member State may provide to the data subject information concerning any of the data subject's personal data that are being processed only if it first gives the issuing Member State an opportunity to state its position. If the personal data was entered in SIS by Europol, the Member State that received the request shall refer the request to Europol without delay, and in any case within 5 days of receipt, and Europol shall process the request in accordance with Regulation (EU) 2016/794 and Regulation (EU) 2018/1725. If Europol receives a

request concerning personal data entered in SIS by a Member State, Europol shall refer the request to the alert issuing Member State without delay, and in any case within 5 days of receipt. The communication between those Member States and between the Member States and Europol shall be carried out through the exchange of supplementary information.

(3) A Member State in accordance with its national law, including law transposing Directive (EU) 2016/680 and, in the case of personal data entered in SIS under Article 37a of this Regulation, Europol in accordance with Chapter IX of Regulation (EU) 2018/1725, shall take a decision not to provide information to the data subject, in whole or in part, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

In cases referred to in the first subparagraph, the Member State or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine any of the reasons set out in points (a) to (e) of the first subparagraph of this paragraph. The Member State or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.

The Member State, or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall document the factual or legal reasons on which the decision not to provide information to the data subject is based. That information shall be made available to the competent supervisory authorities. For such cases, the data subject shall also be able to exercise his or her rights through the competent supervisory authorities.

(4) Following an application for access, rectification or erasure, the Member State or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall inform the data subject about the follow-up given to the exercise of the rights under this Article without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Member State or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall, where possible, be provided by electronic means unless otherwise requested by the data subject. ’

(11) Article 68 is replaced by the following:

‘*Article 68*
Remedies

(1) Without prejudice to the provisions on remedies of Regulation (EU) 2016/679 and of Directive (EU) 2016/680, any person may bring an action before any competent supervisory authority or a court, under the law of any Member State to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her.

(2) Without prejudice to the provisions on remedies of Regulation (EU) 2018/1725, any person may lodge a complaint with the European Data Protection Supervisor in order to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her entered by Europol.

(3) The Member States and Europol undertake mutually to enforce final decisions handed down by the courts, authorities or bodies referred to in paragraphs 1 and 2 of this Article, without prejudice to Article 72.

(4) Member States and Europol shall report annually to the European Data Protection Board on:

(a) the number of access requests submitted to the data controller and the number of cases where access to the data was granted;

(b) the number of access requests submitted to the supervisory authority and the number of cases where access to the data was granted;

(c) the number of requests for the rectification of inaccurate data and for the erasure of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;

(d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the supervisory authority;

(e) the number of court proceedings initiated;

(f) the number of cases where the court ruled in favour of the applicant;

(g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts entered by the issuing Member State or Europol.

A template for the reporting referred to in this paragraph shall be included in the SIRENE Manual.

(5) The reports from the Member States and Europol shall be included in the joint report referred to in Article 71(4).’

(12) Article 72 is replaced by the following:

‘Article 72
Liability

(1) Without prejudice to the right to compensation and to any liability under Regulation (EU) 2016/679, Directive (EU) 2016/680, Regulation (EU) 2018/1725 and Regulation (EU) 2016/794:

(a) any person or Member State that has suffered material or non-material damage, as a result of an unlawful personal data processing operation through the use of

N.SIS or any other act incompatible with this Regulation by a Member State, shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol incompatible with this Regulation shall be entitled to receive compensation from Europol;

(c) any person or Member State that has suffered material or non-material damage as a result of any act by eu-LISA incompatible with this Regulation shall be entitled to receive compensation from eu-LISA.

A Member State, Europol or eu-LISA shall be exempted from their liability, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

(2) If any failure of a Member State or Europol to comply with its obligations under this Regulation causes damage to SIS, that Member State or Europol shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in SIS failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

(3) Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of that Member State. Claims for compensation against Europol for the damage referred to in paragraphs 1 and 2 shall be governed by Regulation (EU) 2016/794 and subject to the conditions provided for in the Treaties. Claims for compensation against eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.'

(13) In Article 74, paragraph 3 is replaced by the following:

'3. eu-LISA shall produce daily, monthly and annual statistics showing the number of records per category of alerts, both for each Member State, Europol and in aggregate. eu-LISA shall also provide annual reports on the number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert, both for each Member State, Europol and in aggregate. The statistics produced shall not contain any personal data. The annual statistical report shall be published.'

(14) In Article 79, the following paragraph 7 is inserted:

'7. The Commission shall adopt a decision setting the date on which Europol shall start entering, updating and deleting data in SIS pursuant to this Regulation as amended by Regulation [XXX], after verification that the following conditions have been met:

(a) the implementing acts adopted pursuant to this Regulation have been amended to the extent necessary for the application of this Regulation as amended by Regulation [XXX];

(b) Europol has notified the Commission that it has made the necessary technical and procedural arrangements to process SIS data and exchange supplementary information pursuant to this Regulation as amended by Regulation [XXX];

(c) eu-LISA has notified the Commission of the successful completion of all testing activities with regard to CS-SIS and to the interaction between CS-SIS and the technical interface of Europol referred to in Article 48(1) of this Regulation as amended by Regulation [XXX].

This decision shall be published in the *Official Journal of the European Union*.'

Article 2
Entry into force

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

It shall apply from the date determined in accordance with Article 79 (7) of Regulation (EU) 2018/1862.

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 'AGENCIES'

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal

1.2. Policy area concerned

1.3. The proposal relates to

1.4. Objectives

1.5. Grounds for the proposal

1.6. Duration and financial impact of the proposal

1.7. Management mode 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

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

3.2. Estimated impact on expenditure

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT 'AGENCIES'

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters.

1.2. Policy area concerned

Policy area: Home Affairs

Activity: Migration and Border Management

Nomenclature: 11 10 02

1118.0207: Border Management - European Agency for the management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)

1.3. The proposal relates to

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[43]

☒ **the extension of an existing action**

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

1.4. Objectives

1.4.1. General objectives

In response to pressing operational needs and calls by the co-legislators for stronger support to Europol, the Commission Work Programme for 2020 announced a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation".

One of the elements of this legislative initiative is to address Europol's limitations in sharing Europol's analysis of data received from third countries and international organisations directly and in real-time with frontline officers in Member States. The proposal to amend Regulation (EU) 2018/1862 on SIS contributes to this initiative by extending the scope of SIS with the creation of a new separate alert category to be used by Europol to share such data, under strict conditions, with frontline officers in Member States.

This is a key action of the July 2020 EU Security Union Strategy. In line with the call by the Political Guidelines to "leave no stone unturned when it comes to protecting our citizens", the initiative is expected to reinforce Europol to help Member States keeping citizens safe.

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

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

1. for Europol to support and strengthen action by the Member States' law enforcement authorities and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy ;

2. for eu-LISA to support Europol and Member States in the exchange of information for the purpose of preventing serious crime or terrorism.

1.4.2. Specific objective

The specific objective derives from the general objectives outlined above: "providing frontline officers with the result of Europol's analysis of data received from third countries."

The aim is to provide frontline officers with the result of Europol's analysis of data received from third countries or international organisations on suspects and criminals when and where this is necessary.

The underlying goal is to give frontline officers direct and real-time access to such data when they check a person at the external border or within territory of the EU, to support them in their tasks.

1.4.3. Expected results and impact

The proposal will primarily benefit individuals and society at large by improving Europol's ability to support Member States in countering crime and protecting EU citizens. Citizens will directly and indirectly benefit from lower crime rates, reduced economic damages, and less security related costs.

The proposal does not contain regulatory obligations for citizens/consumers, and does not create additional costs in that regard.

The proposal will create economies of scale for administrations as it will shift the resource implications of the targeted activities from the national level to the EU level. Public authorities in Member States will directly benefit from the proposal thanks to economies of scale leading to savings in administrative costs.

1.4.4. Indicators of performance

The following main indicators will allow the monitoring of the implementation and performance of the specific objectives:

Specific objective: "entry into operation of the updated functionalities of Central SIS by end 2022"

Indicators for Europol:

- the set-up of a technical interface for the entry, update and deletion of alerts in Central SIS;

- the successful completion of tests organised by eu-LISA.

Indicators for eu-LISA:

- the successful completion of comprehensive pre-launch testing at Central level;

- the successful completion of tests with Europol to transmit data to Central SIS and with all Member States and Agencies systems;

- the successful completion of SIRENE tests for the new alert category.

In line with Article 28 of the FFR and to ensure sound financial management, eu-LISA already monitors progress in the achievement of its objectives with performance indicators. The agency currently has 29 Corporate Key Performance Indicators. These indicators are reported in eu-LISA's Consolidated Annual Activity Report, which include a clear monitoring of the target by end of year as well as comparison with the previous year. These indicators will be adapted as needed following adoption of the proposal.

1.5. Grounds for the proposal/initiative

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

The rollout of the implementation of the initiative requires technical and procedural measures at EU and national level, which should start when the revised legislation enters into force.

The relevant resources – in particular human resources - should be ensured in order to support eu-LISA to contribute to Europol's services.

The main requirements following entry into force of the proposal are as follows with regard to the further development of the Central SIS by eu-LISA:

- to develop and implement a new alert category in Central SIS in line with the requirements defined in the regulation;

- to update the technical specifications related to the exchange of supplementary between SIRENE Bureaux and Europol;

- to develop the functionality for Member States and Agencies to carry out searches in the Central System on this alert category;

- to update the functionalities in Central SIS related to reporting and statistics.

1.5.2. Added value of Union involvement

Serious crime and terrorism are of a transnational nature. Therefore, action at national level alone cannot counter them effectively. This is why Member States choose to work together within the framework of the EU to tackle the threats posed by serious crime and terrorism.

The proposal will create significant economies of scale at an EU level, as it will shift tasks and services, which can be performed more efficiently at an EU level, from the national level to eu-LISA and Europol. The proposal therefore provides for efficient solutions to challenges, which would otherwise have to be addressed at higher costs by means of 27 individual national solutions, or to challenges which cannot be addressed at the national level at all in view of their transnational nature.

1.5.3. Lessons learned from similar experiences in the past

The proposal builds on the need to support Europol and Member States in addressing continuously-evolving transnational security challenges beyond the national level alone.

Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Criminals exploit the advantages that the digital transformation, new technologies , globalisation and mobility bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world. The COVID-19 crisis only added to this, as criminals quickly seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities

These evolving security threats call for effective EU level support to the work of national law enforcement authorities. Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol offers to counter serious crime and terrorism.

This proposal also builds on the lessons learned and progress achieved since the entry into force of the 2018 SIS regulations, the developments done by eu-LISA to implement the 2018 SIS Regulations, and the entry into application of the 2018 eu-LISA Regulation, while recognising that the operational importance of the agency's tasks has already changed substantially. The new threat environment has changed the support Member States need and expect among other tasks also from eu-LISA to support Europol to keep citizens safe, in a way that was not foreseeable when the co-legislators negotiated the current Europol mandate.

Previous review of eu-LISA's mandate and the growing demand for services by Member States has shown that eu-LISA's tasks need to be backed by adequate financial and human resources.

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

The proposal responds to the changing security landscape as it will support eu-LISA to equip Europol with the necessary capabilities and tools to support Member States effectively in countering serious crime and terrorism. The Communication "Europe's moment: Repair and Prepare for the Next Generation" [44] underlined the necessity of building a more resilient Union as the COVID-19 crisis "revealed a number of vulnerabilities and a significant increase in certain crimes, such as cybercrime. This shows the need to reinforce the EU Security Union".

The proposal is fully in line with the Commission Work Programme for 2020 which announced a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation"[45]. eu-LISA will contribute to this objective by extending the scope of SIS in order to enable the creation of a new separate alert category by Europol.

This strengthening of Europol's mandate is one of the key actions identified in the July 2020 EU Security Union Strategy[46]. A more effective Europol will ensure that the agency can fully perform its tasks and can assist in reaching the strategic priorities for the Security Union.

In line with the call by the Political Guidelines[47] to "leave no stone unturned when it comes to protecting our citizens", this proposal addresses those areas where stakeholders ask for reinforced support to Europol in order to help Member States keeping citizens safe.

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

The Multiannual Financial Framework proposal for 2021-2027 recognises the need to reinforce eu-LISA in order to increase support to Member States' for effective border management in 2021.

Since 2016 and the last revision of eu-LISA's mandate, the trend has been towards an exponential growth of the agency's data flows and of the demand on its services[48], leading to requests for budget and staff reinforcements above the levels initially programmed.

Since the proposal will introduce important new tasks in eu-LISA Regulation and will also clarify, codify and detail other tasks, hereby extending eu-LISA's capabilities within the context of the treaties, it therefore cannot be covered by a stable level of resources. The proposal needs to be backed by appropriate financial and human reinforcements to be found within Heading 4 "Migration and Border Management" of the MFF 2021-2027.

44 COM(2020) 456 (27.5.2020)

45 COM(2020) 440 final – Annexes 1 to 2 (27.5.2020)

46 COM(2020) 605 final (24.7.2020).

47 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

48 eu-LISA's 2019 operational indicators for the Schengen Information System show that searches and hits have tripled from 6 million in 2014 to 18 million in 2019.

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**

– Implementation with a start-up period from 2021 to 2022,

– followed by full-scale operation.

1.7. Management mode planned[49]

☐ **Direct management** by the Commission through

– ☐ executive agencies

☐ **Shared management** with the Member States

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

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

– ☐the EIB and the European Investment Fund;

– ☒ bodies referred to in Articles 70 and 71;

– ☐ public law bodies;

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

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

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

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

Comments

The baseline for the EU contribution to eu-LISA's budget has been identified based on the MFF Fiche n°68[50] and on the Working Document III accompanying the Draft Budget 2021. The information in this LFS is without prejudice to the adoption of the MFF 2021-2027 and the Budget 2021.

In the absence of a voted MFF 2021-2027 and Budget 2021, the estimated financial impact of the initiative includes only the resources needed in addition to eu-LISA's baseline EU contribution (additional costs compared to the baseline).

[49] 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.

[50] Working document of the commission services – Decentralised agencies and EPPO.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The monitoring and reporting of the proposal will follow the principles outlined in eu-LISA's Regulation[51], Financial Regulation[52] and in line with the Common Approach on decentralised agencies[53] .

eu-LISA must notably send each year to the Commission, the European Parliament and the Council a Single Programming Document containing multi-annual and annual work programmes and resources programming. The Document sets out the objectives, expected results and performance indicators to monitor the achievement of the objectives and the results. eu-LISA must also submit a Consolidated Annual Activity Report to the management board. This report notably includes information on the achievement of the objectives and results set out in the Single Programming Document. The report must also be sent to the Commission, the European Parliament and the Council.

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

Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended accordingly or repealed.

The Commission shall report to the European Parliament, to the Council and to the Management Board on the findings of the evaluation referred to in paragraph 1. The findings of the evaluation shall be made public.

In addition, with regard to the operation of SIS, on the basis of Regulation (EU) 2018/1862, the Commission, Member States and eu-LISA will regularly review and monitor the use of SIS, to ensure that it continues to function effectively and efficiently.

Article 51 of Regulation (EU) 2018/1862 foresees the evaluation of the use of SIS by Europol, carried out by the Commission at least every five years. This evaluation will

[51] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 (OJ L 295/99 of 21.11.2018.

[52] Decision of the Management Board No 2019-198 establishing the Financial Rules of the European Union Agency for the operational management of Large-Scale IT systems in the area of Freedom, Security and Justice (eu-LISA) of 28.08.2019.

[53] https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf

cover the procedures of Europol to enter data in SIS. Europol will have to ensure adequate follow-up to the findings and recommendations stemming from the evaluation. A report on the results of the evaluation and follow-up to it will be sent to the European Parliament and to the Council.

In addition, Regulation (EU) 2018/1862 includes provisions in Article 74(9) for a formal, regular review and evaluation process that will be also applicable to the new alert category introduced by this amendment.

2.2. Management and control system

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

Considering that the proposal impacts the annual EU contribution to eu-LISA, the EU budget will be implemented via indirect management.

Pursuant to the principle of sound financial management, the budget of eu-LISA shall be implemented in compliance with effective and efficient internal control[54]. eu-LISA is therefore bound to implement an appropriate control strategy coordinated among appropriate actors involved in the control chain.

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

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

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

- annual discharge granted by the European Parliament;

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

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

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

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

The following risks are identified:

- potential difficulties for eu-LISA in managing the developments presented in the current proposal in parallel with other ongoing developments (e.g. the Entry-Exit System, the European Travellers Information and Authorisation System, and the upgrades of SIS, VIS and Eurodac);

[54] Article 30 of eu-LISA's Financial Regulation

- dependencies between the preparations to be done by eu-LISA with regard to Central SIS and the preparations to be done by Europol with regard to setting up a technical interface to transmit data to SIS;

- fragmentation of eu-LISA's core business due to multiplication of tasks and requests;

- lack of adequate levels of financial and human resources to match operational needs;

- lack of ICT resources, resulting in delays in necessary core system developments and updates;

- risks related to eu-LISA's processing of personal data and the need to regularly evaluate and adapt procedural and technical safeguards in order to ensure the protction of personal data and fundamental rights.

eu-LISA implements a specific Internal Control Framework based on the Internal Control Framework of the European Commission. The Single Programming Document must provide information on the internal control systems, while the Consolidated Annual Activity Report (CAAR) must contain information on the efficiency and effectiveness of the internal control systems, including as regards risk assessment. The CAAR 2019 reports that, management of the Agency has reasonable assurance that appropriate internal controls are in place and that they are functioning as intended. Throughout the year, the major risks were appropriately identified and managed. This assurance is further confirmed by the results of the internal and external audits performed.

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

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

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

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

The ratio of "control costs/value of the related funds managed" is reported on by the Commission. The 2019 AAR of DG HOME reports 0.28% for this ratio in relation to Indirect Management Entrusted Entities and Decentralised Agencies, including eu-LISA.

The European Court of Auditors confirmed the legality and regularity of eu-LISA's annual accounts for 2018, which implies an error rate below 2%. There are no indications that the error rate will worsen in the coming years.

Moreover, article 80 of eu-LISA's Financial Regulation provides for the possibility for the agency to share an internal audit capability with other Union bodies functioning in the same policy area if the internal audit capability of a single Union body is not cost-effective.

2.3. Measures to prevent fraud and irregularities

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

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

Moreover, as partner DG, DG HOME has developed and implemented its own anti-fraud strategy on the basis of the methodology provided by OLAF. Decentralised agencies, including Europol, fall within the scope of the strategy. DG HOME 2019 AAR concluded that the fraud prevention and detection processes worked satisfactorily and therefore contributed to the assurance on the achievement of the internal control objectives.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[55]	from EFTA countries[56]	from candidate countries[57]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
4	11 10 02 – 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

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

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

[55] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[56] EFTA: European Free Trade Association.

[57] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	4	Migration and border management

eu-LISA: European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice			Year **2021**[58]	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Title 1:	Commitments	(1)	0,160	0,160	0	0	0	0	0	**0,320**
	Payments	(2)	0,160	0,160	0	0	0	0	0	**0,320**
Title 2:	Commitments	(1a)	0	0	0	0	0	0	0	**0**
	Payments	(2a)	0	0	0	0	0	0	0	**0**
Title 3:	Commitments	(3a)	0	1,500						**1,500**
	Payments	(3b)	0	1,500						**1,500**
TOTAL appropriations for eu-LISA	Commitments	=1+1a +3a	0,160	1,660						**1,820**
	Payments	=2+2a +3b	0,160	1,660						**1,820**

[58] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

Heading of multiannual financial framework	5	'Administrative expenditure'

EUR million (to three decimal places)

		Year N	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
DG: <…….>									
• Human Resources									
• Other administrative expenditure									
TOTAL DG <…….>	Appropriations								

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)								

EUR million (to three decimal places)

		Year 2021[59]	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	0,160	1,660						**1,820**
	Payments	0,160	1,660						**1,820**

[59] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.2.2. 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 **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
	OUTPUTS																	
	Type [60]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 [61] Development Central System																		
- Output					1	1,500	1										1	**1,500**
- Output																		
- Output																		
Subtotal for specific objective No 1					1	1,500	1										1	**1,500**
SPECIFIC OBJECTIVE No 2 Maintenance Central System																		
- Output																		
Subtotal for specific objective No 2																		
TOTAL COST																		

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

61 As described in point 1.4.2. 'Specific objective(s)…'

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

3.2.3.1. Summary

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

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

EUR million (to three decimal places)

	Year **2021** [62]	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Temporary agents (AD Grades)								
Temporary agents (AST grades)								
Contract staff	0,160	0,160						**0,320**
Seconded National Experts								
TOTAL	**0,160**	**0,160**						**0,320**

Staff requirements (FTE):

	Year **2021** [63]	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Temporary agents (AD Grades)								
Temporary agents (AST grades)								
Contract staff	2	2						
Seconded National Experts								

[62] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

[63] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

TOTAL	**2**	**2**						

Recruitment is planned for 2021, for staff to be available to start the development of Central SIS in due time with a view of ensuring the implementation of the newly created alert category by 2022.

3.2.3.2. Estimated requirements of human resources for the parent DG

– ☐ 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 amounts (or at most to one decimal place)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
• **Establishment plan posts (officials and temporary staff)**							
XX 01 01 01 (Headquarters and Commission's Representation Offices)							
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)**[64]							
XX 01 02 01 (AC, END, INT from the 'global envelope')							
XX 01 02 02 (AC, AL, END, INT and JPD in the Delegations)							
XX 01 04 ***yy***[65] - at Headquarters[66]							
XX 01 04 ***yy***[65] - 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							

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary

64 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations .

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

66 Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	
External staff	

Description of the calculation of cost for FTE units should be included in the Annex V, section 3.

3.2.4. Compatibility with the current multiannual financial framework

– ☒ The proposal/initiative is compatible with the current multiannual financial framework.

– ☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Comments:

The proposal is compatible with the MFF 2021-2027.

No reprogramming of MFF 2021-2027 is planned at this stage; however this does not exclude the possibility of future reprogramming.

The budgetary impact of the additional financial resources for EU-LISA will be offset through a compensatory reduction from programmed spending under Heading 4.

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[67].

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

3.2.5. Third-party contributions

– The proposal/initiative does not provide for co-financing by third parties.

– The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[67] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

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 other revenue

– ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[68]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

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

Specify the method for calculating the impact on revenue.

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