



EUROPEAN
COMMISSION

Brussels, 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Over the course of the last two years, the European Union has been working on simultaneously addressing the separate challenges of migration management, integrated border management of the EU's external borders and the fight against terrorism and cross-border crime. Effective information exchange amongst Member States, and between Member States and the relevant EU agencies, is essential to providing a robust response to those challenges and to building an effective and genuine Security Union.

The Schengen Information System (SIS) is the most successful tool for the effective cooperation of immigration, police, customs and judicial authorities in the EU and the Schengen associated countries. Competent authorities in the Member States such as police, border guards and customs officers need to have access to high quality information about the persons or objects they are checking, with clear instructions about what needs to be done in each case. This large-scale information system is at the very heart of Schengen cooperation and plays a crucial role in facilitating the free movement of people within the Schengen area. It enables competent authorities to enter and consult data on wanted persons, persons who may not have the right to enter or stay in the EU, missing persons – in particular children – and objects that may have been stolen, misappropriated or lost. SIS not only contains information about a particular person or object but also clear instructions for the competent authorities on what to do with that person or object once found.

In 2016, the Commission carried out a comprehensive evaluation¹ of SIS, three years after the entry into operation of its second generation. This evaluation showed that SIS has been a genuine operational success. In 2015, national competent authorities checked persons and objects against data held in SIS on nearly 2.9 billion occasions and exchanged over 1.8 million pieces of supplementary information. Nonetheless, as announced in the Commission Work Programme 2017, building on this positive experience, the effectiveness and efficiency of the system should be further strengthened. To this end, the Commission is presenting a first set of three proposals to improve and extend the use of SIS as result of the evaluation while continuing its work to make existing and future law enforcement and border management systems more interoperable, following up on the ongoing work of the High Level Expert Group on Information Systems and Interoperability.

These proposals cover the use of the system (a) for border management, (b) for police cooperation and judicial cooperation in criminal matters, and (c) for the return of illegally staying third country nationals. The first two proposals together form the legal bases for the establishment, operation and use of the SIS. The proposal for the use of SIS for the return of illegally staying third country nationals supplements the proposal for border management and

¹ Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document. (OJ...).

complements the provisions contained therein. It establishes a new alert category and contributes to the implementation and monitoring of Directive 2008/115/EC².

Due to the variable geometry in Member States' participation in EU policies in the area of freedom, security and justice, it is necessary to adopt three separate legal instruments which will nonetheless work seamlessly together to enable the comprehensive operation and use of the system.

In parallel, with a view to enhancing and improving information management at EU level, in April 2016, the Commission began a process of reflection on "Stronger and Smarter Information Systems for Borders and Security".³ The overarching objective is to ensure that competent authorities systematically have the necessary information from different information systems at their disposal. In order to achieve this objective, the Commission has been reviewing the existing information architecture to identify information gaps and blind spots that result from shortcomings in the functionalities of existing systems, as well as from fragmentation in the EU's overall architecture of data management. The Commission set up a High Level Expert Group on Information Systems and Interoperability to support this work, whose interim findings have also informed this first set of proposals as regards issues of data quality.⁴ President Juncker's State of the Union address in September 2016 also referred to the importance of overcoming the current shortcomings in information management and of improving the interoperability and interconnection between existing information systems.

Following the findings of the High Level Expert Group on Information Systems and Interoperability, which will be presented in the first half of 2017, the Commission will consider a second set of proposals to further improve interoperability of SIS with other IT systems in mid-2017. The review of Regulation (EU) No 1077/2011⁵ concerning the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) is an equally important element of this work and is likely to be the subject of separate Commission proposals also in 2017. Investing in swift, effective and qualitative information exchange and information management and ensuring the interoperability of EU databases and information systems is an important aspect of addressing current security challenges.

The current legal framework of the second generation of SIS – concerning its use for the purposes of border checks of third-country nationals is based upon a former first pillar instrument, namely Regulation (EC) No 1987/2006⁶. This proposal replaces⁷ the current legal instrument in order to:

² Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

³ COM(2016) 205 final of 6.4.2016.

⁴ Commission Decision 2016/C 257/03 of 17.6.2016.

⁵ Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

⁶ Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).

⁷ Please see Section 2 'Choice of the instrument' for explanation as to why a replacement rather than a recast of the current legislation was pursued.

- make it compulsory for Member States to enter an alert in SIS in all cases where an entry ban has been issued to an illegally staying third country national in accordance with provisions respecting Directive 2008/115/EC;
- harmonise national procedures for the use of SIS with regard of the consultation procedure to avoid that a third-country national who is subject to an entry ban, holds a valid residence permit issued by a Member State;
- introduce technical changes to improve security and help reduce administrative burdens;
- address the complete end-to-end use of SIS, covering not only the central and national systems, but also the needs of the end-user by ensuring that end-users receive all necessary data to perform their tasks and they comply with all security rules when they process SIS data.

The proposals develop and improve the existing system, rather than establishing a new one. The revision of the SIS will support and strengthen the European Union actions under the European Agendas of Migration and Security, and implements:

- (1) consolidation of the results of the work on the implementation of SIS carried out in the last three years entailing technical amendments to the Central SIS in order to extend some of the existing alert categories and provide new functionalities;
- (2) recommendations for technical and procedural changes resulting from a comprehensive evaluation of the SIS⁸;
- (3) requests from SIS end-users for technical improvements; and
- (4) the interim findings of the High Level Expert Group on Information Systems and Interoperability⁹ as regards data quality.

In light of the fact that this proposal is intrinsically linked to the Commission proposal for a Regulation on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters, a number of provisions are common to both texts. These include measures covering the end-to-end use of SIS, including not only the operation of the central and national systems, but also end-user needs; strengthened measures for business continuity; measures addressing data quality, data protection and data security, and provisions concerning monitoring, evaluation and reporting arrangements. Both proposals also extend the use of biometric information.¹⁰

With the escalation of the migration and refugee crisis in 2015, the need to take effective steps to tackle irregular migration rose considerably. In its *EU Action plan on return*¹¹, the Commission announced that it would propose to make it compulsory for Member States to introduce all entry bans in SIS to help prevent the re-entry into the Schengen area of third country nationals who are not allowed to enter and stay on the territory of the Member States. Entry bans issued in accordance with provisions respecting Directive 2008/115/EC have a

⁸ Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document. (OJ...).

⁹ High Level Expert Group - Chairman's Report of 21 December 2016.

¹⁰ Please see Section 5 'Other elements' for detailed explanation of the changes included in this proposal

¹¹ COM(2015) 453 final.

Schengen-wide effect; hence they can be enforced at the external borders also by authorities of a Member State other than the one that issued the ban. The existing Regulation (EC) No 1987/2006 only allows but does not require Member States to introduce alerts for refusal of entry and stay on the basis of entry bans in SIS. A greater level of effectiveness and harmonisation may be achieved by making it mandatory to enter all entry bans in the SIS.

- **Consistency with existing policy provisions in the policy area as well as with existing and future legal instruments**

This proposal is fully consistent and aligned with the provisions of Directive 2008/115/EC on the issuance and enforcement of entry bans. It therefore complements the existing provisions on entry bans and contributes to the effective enforcement of these bans at the external border, facilitating the application of the obligations defined by the Return Directive and successfully preventing the re-entry of third country nationals concerned in the Schengen area.

- **Consistency with other Union policies**

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

- (1) **Internal security** in relation to the role of SIS for preventing the entry of third-country nationals posing a security threat.

Data protection insofar as this proposal ensures the protection of fundamental rights of individuals whose personal data is processed in SIS.

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

External border management insofar as this proposal assists Member States in controlling their portion of the EU's external borders and in strengthening the effectiveness of the EU system of external border controls.

An effective **EU returns policy** contributing to and enhancing the EU system to detect and prevent the re-entry of third-country nationals following their return. This proposal would help reducing incentives to irregular migration to the EU, one of the main objectives of the European Agenda on Migration¹².

European Border and Coast Guard as regards (i) the possibility for the Agency staff conducting risk analyses and (ii) the access to SIS of the ETIAS Central Unit within the Agency for the purposes of the proposed European Travel Information and Authorisation System (ETIAS)¹³, as well as (iii) for providing a technical interface for SIS access to European Border and Coast Guard Teams, teams of staff involved in return-related tasks and members of the migration management support teams to, within their mandate, have the right to access and search data entered in SIS.

Europol - broader rights to access and search the SIS data, within its mandate, is proposed.

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

Entry/Exit System which proposed a combination of fingerprint and facial image as biometric identifiers for the operation of the Entry/Exit System (EES); an approach that this proposal seeks to reflect.

ETIAS which proposed a thorough security assessment, including a verification in SIS, of visa-exempted third country nationals who intend to travel in the EU.

¹² COM(2015) 240 final.

¹³ COM(2016) 731 final.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The proposal uses Articles 77(2)(b) and (d) as well as 79(2)(c) of the Treaty on the Functioning of the European Union as the legal bases for provisions in the field of integrated border management and illegal immigration.

- **Variable geometry**

This proposal builds upon the provisions of the Schengen *acquis* related to border checks. Therefore the following consequences in relation to the various protocols and agreements with associated countries have to be considered:

Denmark: According to Article 4 of Protocol 22 on the position of Denmark annexed to the Treaties, Denmark shall decide, within a period of six months after the Council has decided on this Regulation, whether it will implement this proposal, which builds upon the Schengen *acquis*, in its national law.

United Kingdom and Ireland: In accordance with Articles 4 and 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union and Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland, and 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*, the United Kingdom and Ireland do not take part in Regulation (EU) 2016/399 (Schengen Borders Code) nor in any other of the legal instruments which are commonly known as the "Schengen *acquis*", viz. the legal instruments organising and supporting the abolition of controls at internal borders and the flanking measures regarding the controls at external borders. This Regulation constitutes a development of this *acquis*, and therefore, the United Kingdom and Ireland are not taking part in the adoption of this Regulation and are not bound by it or subject to its application.

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. This Regulation has to be read in conjunction with Council Decision 2010/365/EU of 29 June 2010¹⁴ which rendered applicable, subject to some restrictions, the provisions of the Schengen *acquis* related to the Schengen Information System in Bulgaria and Romania.

Cyprus and Croatia: This Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession and Article 4(2) of the 2011 Act of Accession.

Associated Countries: On the basis of the respective agreements associating those countries with the implementation, application and development of the Schengen *acquis*, Iceland, Norway, Switzerland and Liechtenstein are to be bound by the Regulation proposed.

¹⁴ Council Decision 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).

- **Subsidiarity**

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). A full subsidiarity analysis has been carried out in previous occasions; this initiative aims at further refining the existing provisions, addressing identified gaps and improving operational procedures.

This considerable level of information exchange between Member States 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 encompass, inter alia, technical improvements to enhance the efficiency of SIS, as well as efforts to harmonise the use of the system across all participating Member States. Due to the transnational nature of these aims and of the challenges in ensuring effective information exchange to counter ever diversifying threats, the EU is well placed to propose solutions to these issues, which cannot be sufficiently achieved by the Member States alone.

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 impeding the work of competent authorities. As an example, the lack of harmonised rules on the deletion of redundant alerts within the system can lead to the hindrance of free movement of persons as a fundamental principle of the Union.

- **Proportionality**

Article 5 of the Treaty on the European Union states that action by the Union shall not go beyond what is necessary to achieve the objectives set out in the Treaty. The form chosen for this EU action must enable the proposal to achieve its objective and be implemented as effectively as possible. The proposed initiative constitutes a revision of SIS in relation to border checks.

The proposal is driven by the *privacy by design* principles. In terms of the right to protection of personal data, this proposal is proportionate as it provides for 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 contain only the data that is required to identify and locate a person or an object and to enable appropriate operational action to be taken. 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. It also includes provisions designed specifically to strengthen the security of individuals' personal data held in SIS.

No further processes or harmonisation will be necessary at EU level to make the system work. 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.

- **Choice of the instrument**

The proposed revision will also take the form of a Regulation and will replace Regulation (EC) No 1987/2006. This approach has also been followed in relation to Council Decision 2007/533/JHA and, as both instruments are intrinsically linked, it has to be applied in relation to Regulation (EC) No 1987/2006 as well. Decision 2007/533/JHA was adopted as a so-called 'third pillar instrument' under the former Treaty on the European Union. Such 'third pillar' instruments were adopted by the Council without the European Parliament as co-legislator. The legal basis of this proposal is in the Treaty on the Functioning of the European Union (TFEU) since the pillar structure ceased to exist with the entry into force of the Lisbon Treaty on 1 December 2009. The legal basis commands the use of the ordinary legislative procedure. 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.

The proposal will build on and enhance an existing centralised system through which Member States cooperate with each other, something which requires a common architecture and binding operating rules. Moreover, it lays down mandatory rules on access to the system including for the purpose of law enforcement which are uniform for all Member States as well as the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice¹⁵ (eu-LISA). Since 9 May 2013, eu-LISA is responsible for the operational management Central SIS, which consists of all tasks necessary to ensure the full operation of Central SIS 24 hours a day, 7 days a week. This proposal builds on the responsibilities of eu-LISA in relation to SIS.

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

- **Ex-post evaluations/fitness checks of existing legislation**

In accordance with the Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA¹⁶, three years after its entry into operation, the Commission carried out an overall evaluation of the central SIS II system as well as of the bilateral and multilateral exchange of supplementary information between Member States.

The evaluation specifically targeted the review of the application of Article 24 of Regulation (EC) No 1987/2006 with the purpose of making necessary proposals to modify the provisions of this Article to achieve a greater level of harmonisation of the criteria for entering alerts.

The results of the evaluation highlighted the need for changes to the SIS legal basis in order to provide a better response to new security and migration challenges. This includes for example a proposal for the mandatory entry of entry bans into SIS to better enforce them, the

¹⁵ Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

¹⁶ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

mandatory consultation between Member States to avoid the co-existence of an entry ban and a residence permit, the option to identify and locate individuals on the basis of their fingerprints through the use of a new automated fingerprint identification system, and expanding the biometric identifiers in the system.

The evaluation results also showed the need for legal amendments in order to improve the technical functioning of the system and to streamline national processes. These measures will enhance the efficiency and effectiveness of SIS by facilitating its use and reducing unnecessary burden. Further measures are designed to enhance the data quality and transparency of the system by more clearly describing the specific reporting tasks of member States and eu-LISA.

The results of the comprehensive evaluation (the evaluation report and the related Staff Working Document were adopted on 21 December 2016¹⁷) have formed the basis of the measures contained within this proposal.

Furthermore, in accordance with Article 19 of the Return Directive 2008/115/EC, the Commission published a Communication on EU Return Policy in 2014¹⁸, which reports on the application of that Directive. It concluded that the potential of SIS in the field of return policy should be further enhanced; it indicates that the review of SIS II is an opportunity to improve consistency between the return policy and SIS II, and it suggests introducing an obligation on Member States to enter a refusal of entry alert in SIS II for entry bans issued under the Return Directive.

- **Stakeholder consultations**

During the Commission's evaluation of SIS, feedback and suggestions were sought from relevant stakeholders, including delegates to the SISVIS Committee under the procedure established in Article 51 of Regulation (EC) No 1987/2006. This Committee includes the Member States' representatives on both operational SIRENE matters (cross-border cooperation in relation to SIS) and technical matters in the development and maintenance of SIS and the related SIRENE application.

Delegates responded to detailed questionnaires as part of the evaluation process. Where further clarification was necessary or the subject needed to be further developed this was achieved through email exchange or targeted interview.

This iterative process allowed issues to be raised in a comprehensive and transparent way. Throughout 2015 and 2016, delegates to the SISVIS Committee discussed these issues in dedicated meetings and workshops.

The Commission also consulted specifically with Member State national data protection authorities and members of the SIS II Supervision Coordination Group in the field of data protection. Member States shared their experiences on subject access requests and the work of national data protection authorities by responding to a dedicated questionnaire. The responses to this questionnaire from June 2015 have informed the development of this proposal.

¹⁷ Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document.

¹⁸ COM(2014) 199 final.

Internally, the Commission set up an Inter-service Steering Group including the Secretariat-General and the Directorates-General for Migration and Home Affairs, Justice and Consumers, Human Resources and Security, and Informatics. This steering group monitored the evaluation process and provided guidance as needed.

The evaluation's findings also took into account evidence collected during on-site evaluation visits to Member States, examining in detail how SIS is being used in practice. This includes discussions and interviews with practitioners, SIRENE Bureau staff and national competent authorities.

Feedback and suggestions of Member States' competent return authorities, notably on the consequences of a possible obligation to introduce alerts in SIS for all entry bans issued in accordance with Directive 2008/115/EC, were also sought in the context of the Commission's Contact Group Return Directive, during its meetings on 16 November 2015, 18 March and 20 June 2016.

In light of this feedback, this proposal makes provision for measures to improve the technical and operational efficiency and effectiveness of the system.

- **Collection and use of expertise**

In addition to the stakeholder consultations, the Commission also sought external expertise via four studies, the findings of which have been incorporated in the developments of this proposal:

- SIS Technical Assessment (Kurt Salmon)¹⁹

This assessment identified the key issues in the functioning of SIS and future needs that should be addressed, primarily identifying concerns with regards to maximising business continuity and ensuring that the overall architecture can adapt to increasing capacity requirements.

- ICT Impact Assessment of Possible Improvements to the SIS II Architecture (Kurt Salmon)²⁰

This study assessed the current cost of operating the SIS at national level and to evaluated two possible technical scenarios for the improvement of the system. Both scenarios include a set of technical proposals focusing on improvements to the central system and overall architecture.

- "ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report", 10 November 2016, (Wavestone)²¹

This study assessed the cost impacts on Member States of the implementation of a national copy by analysing three scenarios (a fully centralised system, a standardised N.SIS implementation developed and provided by eu-LISA to Member States and a distinct N.SIS implementation with common technical standards).

¹⁹ European Commission FINAL REPORT — SIS II technical assessment.

²⁰ European Commission FINAL REPORT — ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016.

²¹ European Commission FINAL REPORT — ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report", 10 November 2016, (Wavestone).

- Study on the feasibility and implications of setting up within the framework of the Schengen Information System an EU-wide system for exchanging data on and monitoring compliance with return decisions (PwC)²²

This study assesses the feasibility and the technical and operational implications of the proposed changes to the SIS with the purpose of enhancing its use for the return of irregular migrants and for preventing their re-entry.

- **Impact assessment**

The Commission did not carry out an impact assessment.

The three independent assessments mentioned above formed the basis of consideration for the impacts of changes to the system from a technical perspective. In addition, the Commission has concluded two reviews of the SIRENE Manual since 2013, i.e. since SIS II entered into operation on 9 April 2013 and Decision 2007/533/JHA became applicable. This includes a mid-term review assessment which resulted in the launch of a new SIRENE Manual²³ on 29 January 2015. The Commission also adopted a Catalogue of Best Practices and Recommendations²⁴. Moreover, eu-LISA and the Member States carry out regular, iterative technical improvements to the system. It is considered that these options have now been exhausted, requiring more wholesale amendment to the legal basis. Clarity in areas such as application of end-user systems as well as detailed rules on alert deletion cannot be achieved through improved implementation and enforcement alone.

Furthermore, the Commission has carried out a comprehensive evaluation of SIS as it was required by Articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and published an accompanying Staff Working Document. The results of the comprehensive evaluation (the evaluation report and the related Staff Working Document were adopted on 21 December 2016) have formed the basis of the measures contained within this proposal.

The Schengen evaluation mechanism, laid down in Regulation (EU) No. 1053/2013²⁵ allows the periodic legal and operational assessment of the functioning of SIS in the Member States. The evaluations are jointly carried out by the Commission and Member States. Through this mechanism, the Council makes recommendations to individual Member States, based on the evaluations carried out as part of multi-annual and annual programmes. As a result of their individual nature, these recommendations cannot replace legally binding rules which are applicable at the same time to all Member States using the SIS.

²² Study on the feasibility and implications of setting up within the framework of the SIS and EU-wide system for exchanging data on and monitoring compliance with return decisions, 4 April 2015, PwC.

²³ Commission Implementing Decision (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (OJ L 44, 18.2.2015, p. 75).

²⁴ Commission recommendation establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS II (C(2015)9169/1).

²⁵ Regulation (EU) No. 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p.27).

The SISVIS Committee regularly discusses practical operational and technical issues. Although these meetings are instrumental in the cooperation between the Commission and the Member States, the outcome of these discussions (absent legislative changes) cannot remedy issues emerging due to diverging national practices, for example.

The changes proposed in this Regulation do not present a significant economic or environmental impact. However, these changes are expected to have a significantly positive social impact, as they provide for increased security by allowing for better identification of persons using false identities, criminals whose identity remains unknown after having committed a serious crime as well irregular migrants taking advantage of the area without internal border controls. The impact of these changes on fundamental rights and data protection has been considered and set out in more detail in the next section ("Fundamental rights").

The proposal has been drawn up making use of the substantial body of evidence collected to inform the overall evaluation of the second generation of SIS, which explored the functioning of the system and possible areas for improvement. In addition, a cost impact assessment study was carried out, to ensure that the national architecture chosen was the most appropriate and proportionate.

- **Fundamental rights and data protection**

This proposal develops and improves an existing system, rather than establishing a new one, and hence builds upon important and effective safeguards that have already been put in place. Nevertheless, as the system continues to process personal data, and will process further categories of sensitive biometric data, 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 collection and further processing of data to what is strictly necessary and operationally required, and restricting access to that data to those who have an operational need to process it. Clear data retention timeframes have been set out in this proposal, and there is explicit recognition of and provision for individuals' rights to access and rectify data relating to them and to request erasure in line with their fundamental rights (see section on data protection and security).

In addition, the proposal strengthens measures to protect fundamental rights, as it sets out in legislation the requirements for an alert to be deleted and introduces a proportionality assessment if an alert is being extended. The proposal defines extensive and robust safeguards for the use of biometric identifiers to avoid innocent persons being inconvenienced.

The proposal also requires the end-to-end security of the system, ensuring greater protection for the data stored within it. With the introduction of a clear incident management procedure, as well as improved business continuity for the SIS, this proposal fully complies with the Charter of Fundamental Rights of the European Union²⁶ not only as regards the right to the protection of personal data. The development and continued effectiveness of SIS will contribute to the security of persons within society.

The proposal envisages significant changes concerning biometric identifiers. In addition to fingerprints, palm prints should also be collected and stored if the legal requirements are met. Fingerprint logs are attached to alphanumeric SIS alerts as provided for in Article 24. It should be possible in the future to search these dactylographic data (fingerprints and palm

²⁶ Charter of Fundamental Rights of the European Union (2012/C 326/02).

prints) with fingerprints found at a scene of crime provided that the offence qualifies as serious crime or terrorist offence and that it can be to a high degree of probability that they belong to the perpetrator. In case of uncertainty concerning a person's identity based upon his documents, the competent authorities should carry out a fingerprint against the fingerprints stored in the SIS database.

The proposal requires the collection and storage of additional data (such as details of the personal identification documents) that facilitate the work of the officers on the ground to establish the identity of a person.

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

SIS constitutes one single information system. Consequently, the expenditures foreseen in two of the proposals (the current one and the Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters) should not be considered as two separate amounts but as a single one. The budgetary implications of the changes required for the implementation of both proposals are included in one legislative financial statement.

Due to the complementary nature of the third proposal (concerning the return of illegally staying third country nationals) the budgetary implications are dealt with separately and in an independent financial statement addressing only the establishment of this specific alert category.

On the basis of an assessment of the various aspects of the work required in relation to the network, the Central SIS by eu-LISA and the national developments in the Member States, the two proposals for Regulations will require a global amount of EUR 64.3 million for the period 2018-2020.

This covers an increase of the TESTA-NG bandwidth due to the fact that in accordance with the two proposals, the network will transmit fingerprint files and facial images requiring higher throughput and capacity (EUR 9.9 million). It also covers eu-LISA's costs in relation to staff and operational expenditure (EUR 17.6 million). eu-LISA informed the Commission that the recruitment of 3 new contract agents is planned to take place in January 2018 to start the development phase in due time to ensure entry into operations of the updated functionalities of SIS in 2020. The present proposal entails technical amendments to the Central SIS in order to extend some of the existing alert categories and provide new functionalities. The financial statement attached to this proposal reflects these changes.

Furthermore, the Commission carried out a cost impact assessment study to assess the costs of the national developments necessitated by this proposal.²⁷ The estimated cost is EUR 36.8 million which should be distributed via a lump sum to the Member States. Hence, each Member State will receive the amount of EUR 1.2 million to upgrade its national system in

²⁷ Wavestone "ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report", 10 November 2016, Scenario 3 Distinct N. SIS II Implementation.

accordance with the requirements set out in this proposal, including for setting up a partial national copy where this is not yet the case or for a back-up system.

A re-programming of the remainder of the Smart Borders envelope of the Internal Security Fund is planned in order to carry out the upgrades and implement the functionalities foreseen in the two proposals. The ISF Borders Regulation²⁸ is the financial instrument where the budget for the implementation of the Smart Borders package has been included. Article 5 of the Regulation provides that EUR 791 million shall be implemented through a programme for setting up IT systems supporting the management of migration flows across the external border under the conditions laid down in Article 15. Out of the above-mentioned EUR 791 million, EUR 480 million is reserved for the development of the Entry-Exit System and EUR 210 million for the development of the European Travel Information and Authorisation System (ETIAS). The remainder will be partly used to cover the costs of the changes foreseen in the two proposals concerning SIS.

5. OTHER ELEMENTS

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

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 SISVIS Committee to implement technical and operational measures as described in the proposal.

In addition, this proposed Regulation includes provision in Article 54(7) and (8) for a formal, regular review and evaluation process.

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.

Furthermore, 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.

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

²⁸ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa (OJ L 150, 20.5.2014, p. 143).

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

Provisions that are common to this proposal and the proposal for a Regulation on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters:

- General Provisions (Articles 1 – 3)
- Technical architecture and ways of operating SIS (Articles 4 – 14)
- Responsibilities of eu-LISA (Articles 15 – 18)
- Right to access and retention of alerts (Articles 29, 30, 31, 33 and 34)
- General data processing and data protection rules (Articles 36 – 53)
- Monitoring and statistics (Article 54)

End-to-end use of SIS

With over 2 million end-users in the competent authorities across Europe, SIS is an extremely widely used and effective tool for information exchange. These proposals include rules covering the complete end-to-end operation of the system, including Central SIS operated by eu-LISA, the national systems and the end-user applications. It addresses not only the central and national systems themselves, but also the end-users' technical and operational needs.

Article 9(2) specifies that end-users must receive the data required to perform their tasks (in particular all data required for the identification of the data subject and to take the required action). It also provides for a common blueprint for Member State implementation of SIS, ensuring harmonisation across all national systems. Article 6 stipulates that each Member State must ensure uninterrupted availability of SIS data to end-users, in order to maximise the operational benefits by reducing the possibility of downtime.

Article 10(3) ensures that the security of data processing also includes the data processing activities of the end-user. Article 14 obliges Member States to ensure that staff with access to SIS receive regular and ongoing training about data security and data protection rules.

As a result of the inclusion of these measures, this proposal more comprehensively covers the full end-to-end functioning of the SIS, with rules and obligations concerning the millions of end-users across Europe. In order to use SIS to its full effectiveness Member States should ensure that each time their end-users are entitled to carry out a search in a national police or immigration database, they also search SIS in parallel. This way SIS can fulfil its objective as the main compensatory measure in the area without internal border controls and Member States can better address the cross-border dimension of criminality and the mobility of criminals. This parallel search must remain in compliance with Article 4 of Directive (EU) 2016/680²⁹.

Business continuity

²⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJ L 119, 4.5.2016, p.89).

The proposals strengthen provisions regarding business continuity, both at national level and for eu-LISA (Articles 4, 6, 7 and 15). These ensure that SIS will continue to remain functional and accessible to staff on the ground, even if there are issues that affect the system.

Data quality

The proposal maintains the principle that the Member State, which is the data owner, is also responsible for the accuracy of the data entered in SIS (Article 39). It is, however, necessary to provide for a central mechanism managed by eu-LISA which allows Member States to regularly review those alerts in which the mandatory data fields may raise quality concerns. Therefore Article 15 of the proposal empowers eu-LISA to produce data quality reports to Member States at regular intervals. This activity may be facilitated by a data repository for producing statistical and data quality reports (Article 54). These improvements reflect the interim findings of the High Level Expert Group on Information Systems and Interoperability.

Photographs, facial images, dactylographic data and DNA profiles

The possibility to search with fingerprints with a view to identify a person is already set out in Article 22 of Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA. The proposals make this search mandatory if the identity of the person cannot be ascertained in any other way. Currently, facial images can only be used to confirm a person's identity following an alphanumeric search, rather than as the basis for a search. Furthermore, changes to Articles 22 and 28 make provision for facial images, photographs and palm prints to be used to search the system and identify people, when this becomes technically possible. Dactylography refers to the scientific study of fingerprints as a method of identification. Experts in dactylography recognise that palm prints have the characteristic of uniqueness and that they contain reference points that enable accurate and conclusive comparisons just as do fingerprints. Palm prints can be used to establish a person's identity in the same way that fingerprints can be used. The taking of palm prints along with the ten rolled and ten flat prints of a person has been police practice for many decades. There is one main use of palm prints, namely for identification purposes when the subject has intentionally or unintentionally damaged the tips of their fingers. This can be through an attempt to avoid being identified or fingerprinted or through damage caused by accident or heavy manual work. In the course of the discussion on the technical rules of SIS AFIS, Member States reported considerable success in the identification of irregular migrants who had intentionally damaged their fingertips in an attempt to avoid identification. The taking of palm prints by Member State authorities allowed subsequent identification.

The use of facial images for identification will ensure greater consistency between SIS and the proposed EU Entry Exit System, electronic gates and self-service kiosks. This functionality will be limited to the regular border crossing points.

Access by authorities to SIS – institutional users

This sub-section is intended to describe the new elements in access rights with regard to EU Agencies (institutional users). The access rights of competent national authorities have not been amended.

Europol (Article 30) and the European Border and Coast Guard Agency – as well as its teams, teams of staff involved in return-related tasks, and members of the migration management support team – and the ETIAS Central Unit within the Agency (Articles 31 and 32) have the access to SIS and SIS data that they need. Appropriate safeguards are put in place to ensure

that the data in the system is properly protected (including also the provisions in Article 33, requiring that these bodies may only access the data they need to carry out their tasks).

These changes extend access to SIS for Europol to refusal of entry alerts, ensuring that it can make best use of the system as it carries out its duties, and add new provisions that ensure that the European Border and Coast Guard Agency as well as its teams can access the system while carrying out the different operations under their mandate assisting Member States. Furthermore under Commission proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)³⁰ the ETIAS Central Unit of the European Border and Coast Guard Agency will, via ETIAS, verify against SIS whether the third country national applying for a travel authorisation is subject of a SIS alert. To this end the ETIAS Central Unit will also have access to SIS³¹.

Article 29(3) sets out that national visa authorities may also, in the performance of their tasks, access alerts on documents issued in accordance with the Regulation 2008/.... on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters.

This will allow these bodies to have the access to SIS and SIS data that they need in order to carry out their tasks, while also putting in place appropriate safeguards to ensure that the data in the system is properly protected (including also the provisions in Article 35, requiring that these bodies may only access the data they need to carry out their tasks).

Refusal of entry and stay

Currently, in accordance with Article 24(3) of the SIS II Regulation, a Member State may insert an alert in SIS in respect of persons subject to an entry ban based on a failure to comply with national migration legislation. The revised Article 24(3) requires that an alert be entered in SIS in any case in which an entry ban has been issued to an illegally staying third country national in accordance with provisions respecting Directive 2008/115/EC. It also establishes the timing and conditions for entering such alerts after the third-country national has left the territories of the Member States in compliance with an obligation to return. This provision is inserted in order to avoid that entry bans are visible in SIS while the third-country national concerned is still present on the EU territory. Since entry bans prohibit the re-entry into the territories of the Member States, they can come into effect only after the return of the third-country nationals concerned. At the same time, Member States should take all necessary measure to ensure that there is no time-gap between the moment of return and the activation of the alert on refusal of entry and stay in SIS.

This proposal is closely linked with the Commission proposal³² concerning the use of SIS for the return of illegally staying third country nationals, laying down the conditions and procedures for entering alert on return decisions in SIS. That proposal includes a mechanism for monitoring whether third-country nationals who are the subject of a return decision effectively leave the EU territory and a warning mechanism in case of non-compliance. Article 26 sets out the consultation process that Member States must follow when they encounter alerts on refusal of entry and stay – or are willing to enter such alerts – that collide with other Member States' decisions, such as for instance a valid residence permit. Such rules

³⁰ COM (2016)731 final.

³¹ The ETIAS Central Unit is granted access to Articles 24 and 27 of this Regulation.

³² COM (2016)...

should prevent the emergence of, or resolve, the conflicting instructions that these situations may create, while offering clear guidance to end-users on the actions to be taken in such situations and to Member States authorities on whether an alert should be deleted.

Article 27 (ex-Article 26 of Regulation (EC) No 1987/2006) is intended to implement the EU sanction regime which affects third-country nationals who are subject of a restriction to be admitted to the EU territory in accordance with Article 29 of the Treaty on the European Union. In order to allow entering such alerts it was necessary to require the minimum data necessary for the identification of the person, namely surname and date of birth. The fact that Regulation (EC) No 1987/2006 waived the requirement to enter the date of birth created significant challenges as without a date of birth, no alert can be created in SIS, in line with the technical rules and the search parameters of the system. As Article 27 is indispensable to have an efficient EU sanction regime the proportionality requirement does not apply in this respect.

In order to ensure greater consistency with Directive 2008/115/EC the terminology used when referring to the purpose of the alert ("refusal of entry and stay") has been aligned with the wording used in the Directive.

Distinguishing between persons with similar characteristics

In order to ensure that data is processed and stored appropriately, and to reduce the risk of duplication and misidentification, Article 41 sets out the process to follow if it appears, on entering a new alert, that there is already an entry in SIS with similar characteristics.

Data protection and security

This proposal clarifies responsibility for preventing, reporting and responding to incidents that might affect the security or integrity of SIS infrastructure, SIS data or supplementary information (Articles 10, 16 and 40).

Article 12 contains provisions on keeping and searching logs of the history of alerts.

Article 15(3) maintains Article 15(3) of Regulation (EC) No 1987/2006 and provides that the Commission remains responsible for the contractual management of the communication infrastructure, including tasks relating to the implementation of the budget and the acquisition and renewal. These tasks will be transferred to eu-LISA in the second suite of SIS proposals in June 2017.

Article 21 extends the requirement for Member States to consider proportionality before issuing alerts to also apply to decisions on whether the validity period of an alert should be extended. As a novelty, however, Article 24(2) (c) requires Member States to create an alert in all circumstances, on those persons whose activity falls under Articles 1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism.

Categories of data and data processing

In order to provide more and more precise information to the end-users to facilitate and accelerate the required action as well as to allow the better identification of the alert subject this proposal expands the types of information (Article 20) that can be held about people for whom an alert has been issued, to also include:

- whether the person is involved in any activity falling under Articles 1, 2 , 3 and 4 of Council Framework Decision 2002/475/JHA;
- whether the alert is related to an EU citizen or other person who enjoys rights of freedom of movement equivalent to those of EU citizens;
- whether a decision on refusal of entry is based on provisions in Article 24 or in Article 27;
- the type of offence (for alerts issued under Article 24(2));
- details of a person's identity or travel document;
- colour copy of the person's identity or travel document;
- photographs and facial images;
- fingerprints and palm prints.

Having appropriate data is essential to ensure the accurate identification of a person who is checked at a border crossing, who is subject to an internal check or who applies for permission to stay. An inaccurate identification can result in fundamental rights issues; it can also lead to a situation in which the appropriate follow-up actions cannot be taken as there is no knowledge of the existence or content of an alert.

Concerning the information on the underlying decision, four reasons can be distinguished: a previous conviction as referred to in Article 24 (2)(a), a serious security threat as referred to in Article 24 (2)(b), an entry ban as referred to in Article 24 (3) and a restrictive measure as referred to in Article 27. In order to ensure that appropriate actions are taken in case of a hit it is also necessary to indicate whether the alert is related to an EU citizen or other person who enjoys rights of freedom of movement equivalent to those of EU citizens. Having appropriate data is essential to ensure the accurate identification of a person who is checked at a border crossing, who is subject to an internal check or who applies for permission to stay. An inaccurate identification can result in fundamental rights issues; it can also lead to a situation in which the appropriate follow-up actions cannot be taken as there is no knowledge of the existence or content of an alert.

It also (Article 42) expands the list of personal data that may be entered and processed in SIS for the purpose of dealing with misused identities as more data facilitates the victim and the perpetrator of misused identity. The extension of this provision entails no risk as all these data can only be entered upon the consent of the victim of misused identity. This will now also include:

- facial images;
- palm prints;
- details of identity documents;
- the victim's address;
- the names of the victim's father and mother.

Article 20 provides for more detailed information in the alerts. It includes categories for the reason of the refusal of entry and stay and the details of the personal identification documents of the data subjects. This enhanced information allows for the better identification of the person concerned, and on the other hand for a more informed decision to be taken by the end-users. For the protection of the end-users carrying out the checks, SIS will also show if the

person in relation to whom an alert was issued, falls under any of the categories provided in Articles 1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism³³.

The proposal makes clear that Member States must not copy data entered by another Member State into other national data files (Article 37).

Retention

Article 34 sets out the timeframe for reviewing alerts. The maximum retention period of refusal of entry and stay alerts has been aligned with the possible maximum length of entry bans issued in accordance with Article 11 of Directive 2008/115/EC. Thus, the maximum retention period will become 5 years; Member States may, however, set shorter periods.

Deletion

Article 35 sets out the circumstances under which alerts must be deleted, bringing greater harmonisation to national practices in this area. Article 35 sets out particular provisions for SIRENE Bureau staff to delete alerts that are no longer required proactively that are no longer required if no reply is received from the competent authorities.

Rights for data subjects to access data, rectify inaccurate data and erase unlawfully stored data

The detailed rules on the data subject's rights remained unchanged as the existing rules already ensure a high level of protection and are in line with Regulation (EU) 2016/679³⁴ and Directive 2016/680³⁵. In addition to that Article 48 sets out the circumstances under which Member States may decide not to communicate information to data subjects. This must be for one of the reasons listed in this Article, and it must be a proportionate and necessary measure, in line with national law.

Statistics

In order to maintain an overview of the functioning of remedies, Article 49 makes provision for a standard statistical system providing annual reports on numbers of:

- data subject's access requests;
- requests for rectification of inaccurate data and erasure of unlawfully stored data;
- cases before the courts;
- cases where the court ruled in favour of the applicant; and

³³ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

³⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

³⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJ L 119, 4.5.2016, p.89).

- observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the alert-issuing State.

Monitoring and statistics

Article 54 sets out the arrangements that must be put in place to ensure the proper monitoring of SIS and its functioning against its objectives. To do this, eu-LISA is charged with providing daily, monthly and annual statistics on how the system is being used.

Article 54(5) requires euLISA to provide the Member States, the Commission, Europol and the European Border and Coast Guard Agency with statistical reports that it produces and allows the Commission to request additional statistical and data quality reports relating to SIS and SIRENE communication.

Article 54(6) provides for the creation and hosting of a central repository of data, as part of eu-LISA's work on monitoring the functioning of SIS. This will enable authorised staff of Member States, the Commission, Europol and the European Border and Coast Guard Agency to access the data listed in Article 54(3) in order to produce the statistics required.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty the Functioning of the of the European Union, and in particular Articles 77(2)(b) and (d) and 79(2)(c) 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 the application of the provisions of the Schengen acquis as integrated into the framework of the European Union. SIS is one of the major compensatory measures contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between border guards, police, customs and other law enforcement authorities, judicial authorities in criminal matters and immigration authorities.
- (2) SIS was set up pursuant to the provisions of Title IV of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders³⁶ (the Schengen Convention). The development of the second generation of SIS (SIS II) was entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001³⁷ and Council Decision 2001/886/JHA (SIS)³⁸ and it was established by Regulation (EC) No 1987/2006³⁹ as well as by Council Decision 2007/533/JHA⁴⁰. SIS II replaced SIS as created pursuant to the Schengen Convention.

³⁶ OJ L 239, 22.9.2000, p. 19. Convention as amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).

³⁷ OJ L 328, 13.12.2001, p. 4.

³⁸ Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II) (OJ L 328, 13.12.2001, p. 1).

³⁹ Regulation (EC) No 1987/2006 of 20 December 2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information system (SIS II) (OJ L181, 28.12.2006, p. 4).

- (3) Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system in accordance with Articles 24(5), 43(5) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59 and 65(5) of Decision 2007/533/JHA. The evaluation report and the related Staff Working Document were adopted on 21 December 2016⁴¹. The recommendations set out in those documents should be reflected, as appropriate, in this Regulation.
- (4) This Regulation constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapter 2 of Title V of the Treaty on Functioning of the European Union. Regulation (EU) 2018/... of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters⁴² constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of the Treaty on Functioning of the European Union.
- (5) The fact that the legislative basis necessary for governing SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical.
- (6) It is necessary to specify the objectives of SIS, its technical architecture and its financing, to lay down rules concerning its end-to-end operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, the authorities authorised to access the data, the use of biometric identifiers and further rules on data processing.
- (7) SIS includes a central system (Central SIS) and national systems with a full or partial copy of the SIS database. Considering that SIS is the most important information exchange instrument in Europe, it is necessary to ensure its uninterrupted operation at central as well as at national level. Therefore each Member State should establish a partial or full copy of the SIS database and should set up its backup system.
- (8) It is necessary to maintain a manual setting out the detailed rules for the exchange of certain supplementary information concerning the action called for by alerts. National authorities in each Member State (the SIRENE Bureaux), should ensure the exchange of this information.
- (9) In order to maintain the efficient exchange of supplementary information concerning the action to be taken specified in the alerts, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning available resources, user training and the response time to the inquiries received from other SIRENE Bureaux.
- (10) The operational management of the central components of SIS are exercised by the European Agency for the operational management of large-scale IT systems in the

⁴⁰ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information system (SIS II) (OJ L 205, 7.8.2007, p.63).

⁴¹ Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document.

⁴² Regulation (EU) 2018/...

area of freedom, security and justice⁴³ (the Agency). In order to enable the Agency to dedicate the necessary financial and personal resources covering all aspects of the operational management of Central SIS, this Regulation should set out its tasks in detail, in particular with regard to the technical aspects of the exchange of supplementary information.

- (11) Without prejudice to the responsibility of Member States for the accuracy of data entered into SIS, the Agency should become responsible for reinforcing data quality by introducing a central data quality monitoring tool, and for providing reports at regular intervals to the Member States.
- (12) In order to allow better monitoring of the use of SIS to analyse trends concerning migratory pressure and border management, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the Commission, Europol and the European Border and Coast Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic produced should not contain personal data.
- (13) SIS should contain further data categories to allow end-users to take informed decisions based upon an alert without losing time. Therefore alerts for the purpose of refusal of entry and stay should hold information concerning the decision on which the alert is based. Furthermore, in order to facilitate identification and detect multiple identities, the alert should include a reference to the personal identification document or number and a copy of such document, where available.
- (14) SIS should not store any data used for search with the exception of keeping logs to verify if the search is lawful, for monitoring the lawfulness of data processing, for self-monitoring and for ensuring the proper functioning of N.SIS, as well as for data integrity and security.
- (15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS should also allow for the processing of data concerning individuals whose identity has been misused (in order to avoid inconveniences caused by their misidentification), subject to suitable safeguards; in particular with the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed.
- (16) Member States should make the necessary technical arrangement so that each time the end-users are entitled to carry out a search in a national police or immigration database they also search SIS in parallel in accordance with Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council⁴⁴. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better address the cross-border dimension of criminality and the mobility of criminals.

⁴³ Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

⁴⁴ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016 (OJ L 119, 4.5.2016, p. 89).

- (17) This Regulation should set out the conditions for use of dactylographic data and facial images for identification purposes. The use of facial images for identification purposes in SIS should also help ensure consistency in border control procedures where identification and the verification of identity are required by the use of dactylographic data and facial images. Searching with dactylographic data should be mandatory if there is any doubt concerning the identity of a person. Facial images for identification purposes should only be used in the context of regular border controls in self-service kiosks and electronic gates.
- (18) Fingerprints found at a crime scene should be allowed to be checked against the dactylographic data stored in SIS if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence. Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA⁴⁵ and ‘terrorist offence’ should be offences under national law referred to in Council Framework Decision 2002/475/JHA⁴⁶.
- (19) It should be possible for Member States to establish links between alerts in SIS. The establishment by a Member State of links between two or more alerts should have no impact on the action to be taken, their retention period or the access rights to the alerts.
- (20) A greater level of effectiveness, harmonisation and consistency can be achieved by making it mandatory to enter in SIS all entry bans issued by the competent authorities of the Member States in accordance with procedures respecting Directive 2008/115/EC⁴⁷, and by setting common rules for entering such alerts following the return of the illegally staying third country national. Member States should take all necessary measures to ensure that no time-gap exist between the moment in which the third-country national leaves the Schengen area and the activation of the alert in SIS. This should ensure the successful enforcement of entry bans at external border crossing points, effectively preventing re-entry into the Schengen area.
- (21) This Regulation should set mandatory rules for the consultation of national authorities in case a third country national holds or may obtain a valid residence permit or other authorisation or right to stay granted in one Member State, and another Member State intends to issue or already entered an alert for refusal of entry and stay to the third country national concerned. Such situations create serious uncertainties for border guards, police and immigration authorities. Therefore, it is appropriate to provide for a mandatory timeframe for rapid consultation with a definite result in order to avoid that persons representing a threat may enter to the Schengen area.
- (22) This Regulation should be without prejudice to the application of Directive 2004/38⁴⁸.
- (23) Alerts should not be kept in SIS longer than the time required to fulfil the purposes for which they were issued. In order to reduce the administrative burden on the authorities involved in processing data on individuals for different purposes, it is appropriate to

⁴⁵ Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.07.2002, p. 1).

⁴⁶ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

⁴⁷ Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

⁴⁸ Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States (OJ L 158, 30.4.2004, p.77).

align the maximum retention period of refusal of entry and stay alerts with the possible maximum length of entry bans issued in accordance with procedures respecting Directive 2008/115/EC. Therefore, the retention period for alerts on persons should be a maximum of five years. As a general principle, alerts on persons should be automatically deleted from SIS after a period of five years. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the defined period and keep statistics about the number of alerts on persons for which the retention period has been extended.

- (24) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. In cases of offences pursuant Articles 1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism⁴⁹ an alert should always be created on third country nationals for the purposes of refusal of entry and stay taking into account the high level of threat and overall negative impact such activity may result in.
- (25) The integrity of SIS data is of primary importance. Therefore, appropriate safeguards should be provided to process SIS data at central as well as at national level to ensure the end-to-end security of data. The authorities involved in the data processing should be bound by the security requirements of this Regulation and be subject to a uniform incident reporting procedure.
- (26) Data processed in SIS in application of this Regulation should not be transferred or made available to third countries or to international organisations.
- (27) To enhance the efficiency of the work of the immigration authorities when deciding about the right of third country nationals to enter and stay in the territories of the Member States, as well as about the return of illegally staying third country nationals, it is appropriate to grant them access to SIS under this Regulation.
- (28) Regulation (EU) 2016/679⁵⁰ should apply to the processing of personal data under this Regulation by Member States authorities when Directive (EU) 2016/680⁵¹ does not apply. Regulation (EC) No 45/2001 of the European Parliament and of the Council⁵² should apply to the processing of personal data by the institutions and bodies of the Union when carrying out their responsibilities under this Regulation. The provisions of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Regulation (EC) No 45/2001 should be further specified in this Regulation where necessary. With regard to

⁴⁹ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

⁵⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁵¹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJ L 119, 4.5.2016, p.89).

⁵² Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

processing of personal data by Europol, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement cooperation⁵³ (Europol Regulation) applies.

- (29) In so far as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.
- (30) Both the Member States and the Agency should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues from a common perspective.
- (31) The national independent supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation. The rights of data subjects for access, rectification and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to require annual statistics from Member States.
- (32) The supervisory authorities should ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit should either be carried out by the supervisory authorities, or the national supervisory authorities should directly order the audit from an independent data protection auditor. The independent auditor should remain under the control and responsibility of the national supervisory authority or authorities which therefore should order the audit itself and provide a clearly defined purpose, scope and methodology of the audit as well as guidance and supervision concerning the audit and its final results.
- (33) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. In order to facilitate Europol in carrying out its tasks, in particular within the European Migrant Smuggling Centre, it is appropriate to allow Europol access to the alert categories defined in this Regulation. Europol's European Migrant Smuggling Centre plays a major strategic role in countering the facilitation of irregular migration, it should obtain access to alerts on persons who are refused entry and stay within the territory of a Member State either on criminal grounds or because of non-compliance with entry and stay conditions.
- (34) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial – Member States should share information on terrorism-related activity with Europol in parallel to introducing an alert in SIS, as well as hits and related information. This should allow Europol's European Counter Terrorism Centre to verify if there is any additional contextual information available in Europol's databases and to deliver high quality analysis contributing to disrupting terrorism networks and, where possible, preventing their attacks.

⁵³ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 25.5.2016, p. 53).

- (35) It is also necessary to set out clear rules for Europol on the processing and downloading of SIS data to allow the most comprehensive use of SIS provided that data protection standards are respected as provided in this Regulation and Regulation (EU) 2016/794. In cases where searches carried out by Europol in SIS reveal the existence of an alert issued by a Member State, Europol cannot take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.
- (36) Regulation (EU) 2016/1624 of the European Parliament and of the Council⁵⁴ provides for the purposes of this Regulation, that the host Member State is to authorise the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks, deployed by the European Border and Coast Guard Agency, to consult European databases, where this consultation is necessary for fulfilling operational aims specified in the operational plan on border checks, border surveillance and return. Other relevant Union agencies, in particular the European Asylum Support Office and Europol, may also deploy experts as part of migration management support teams, who are not members of the staff of those Union agencies. The objective of the deployment of the European Border and Coast Guard teams, teams of staff involved in return-related tasks and the migration management support teams is to provide for technical and operational reinforcement to the requesting Member States, especially to those facing disproportionate migratory challenges. Fulfilling the tasks assigned to the European Border and Coast Guard teams, teams of staff involved in return-related tasks and to the migration management support teams, necessitates access to SIS via a technical interface of the European Border and Coast Guard Agency connecting to Central SIS. In cases where searches carried out by the team or the teams of staff in SIS reveal the existence of an alert issued by a Member State, the member of the team or the staff cannot take the required action unless authorised to do so by the host Member State. Therefore it should inform the Member States concerned allowing for follow up of the case.
- (37) In accordance with Regulation (EU) 2016/1624 the European Border and Coast Guard Agency shall prepare risk analyses. These risk analyses shall cover all aspects relevant to European integrated border management, notably threats that may affect the functioning or security of the external borders. Alerts introduced in the SIS in accordance with this Regulation, notably the alerts on refusal of entry and stay are relevant information for assessing possible threats that may affect the external borders and should thus be available in view of the risk analysis which must be prepared by the European Border and Coast Guard Agency. Fulfilling the tasks assigned to the European Border and Coast Guard Agency in relation to risk analysis, necessitates access to SIS. Furthermore, in accordance with Commission proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)⁵⁵ the ETIAS Central Unit of the European Border and Coast Guard Agency will perform verifications in SIS via ETIAS in order to perform the assessment of the applications for travel authorisation which require, inter alia, to ascertain if the third country national applying for a travel

⁵⁴ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251 of 16.9.2016, p. 1).

⁵⁵ COM (2016)731 final.

authorisation is subject of a SIS alert. To this end the ETIAS Central Unit within European Border and Coast Guard Agency should also have access to SIS to the extent necessary to carry out its mandate, namely to all alert categories on third country nationals in respect of whom an alert has been issued for the purposes of entry and stay, and those who are subject to restrictive measure intended to prevent entry or transit through Member States.

- (38) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality and search rules related to biometric identifiers, rules on compatibility and priority of alerts, the adding of flags, links between alerts, setting the expiry date of alerts within the maximum time limit and the exchange of supplementary information. Implementing powers in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications.
- (39) In order to ensure uniform conditions for the implementation of this Regulation implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011⁵⁶. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (police and judicial cooperation) should be the same.
- (40) In order to ensure transparency, a report on the technical functioning of Central SIS and the communication infrastructure, including its security, and on the exchange of supplementary information should be produced every two years by the Agency. An overall evaluation should be issued by the Commission every four years.
- (41) Since the objectives of this Regulation, namely the establishment and regulation of a joint information system and the exchange of related supplementary information, cannot, by their very nature, be sufficiently achieved by the Member States and can therefore 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 of the European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (42) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation seeks to ensure a safe environment for all persons residing on the territory of the European Union and a protection of irregular migrants from exploitation and trafficking by allowing their identification while fully respecting the protection of personal data.
- (43) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six

⁵⁶ Regulation (EU) No182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

months after the Council has decided on this Regulation whether it will implement it in its national law.

- (44) This Regulation constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC⁵⁷; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (45) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC⁵⁸; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (46) 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 association of those two States with the implementation, application and development of the Schengen *acquis*⁵⁹, which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC⁶⁰ on certain arrangements for the application of that Agreement.
- (47) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 4(1) of Council Decisions 2004/849/EC⁶¹ and 2004/860/EC⁶².
- (48) As regards Liechtenstein, this Decision 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*⁶³, which fall within the area referred to in Article

⁵⁷ OJ L 131, 1.6.2000, p. 43.

⁵⁸ OJ L 64, 7.3.2002, p.20.

⁵⁹ OJ L 176, 10.7.1999, p.36.

⁶⁰ OJ L 176, 10.7.1999, p.31.

⁶¹ Council Decision 2004/849/EC of 25 October 2004 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 368, 15.12.2004, p. 26).

⁶² Council Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 370, 17.12.2004, p. 78).

⁶³ OJ L 160, 18.6.2011, p. 21.

1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU⁶⁴ and Article 3 of Council Decision 2011/350/EU⁶⁵.

- (49) 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 Decision 2010/365/EU on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania⁶⁶.
- (50) Concerning Cyprus and Croatia this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession and Article 4(2) of the 2011 Act of Accession.
- (51) The estimated costs of the upgrade of the SIS national systems and of the implementation of the new functionalities, envisaged in this Regulation are lower than the remaining amount in the budget line for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council⁶⁷. Therefore, this Regulation should re-allocate the amount, attributed for developing IT systems supporting the management of migration flows across the external borders, in accordance with Article 5(5)(b) of Regulation (EU) No 515/2014.
- (52) Regulation (EC) No 1987/2006 should therefore be repealed.
- (53) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on ...,

⁶⁴ 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).

⁶⁵ Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

⁶⁶ OJ L 166, 1.7.2010, p. 17.

⁶⁷ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa (OJ L 150, 20.5.2014, p. 143).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

General purpose of SIS

The purpose of SIS shall be to ensure a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Chapter 2 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons in their territories, using information communicated via this system.

Article 2

Scope

1. This Regulation establishes the conditions and procedures for the entry and processing in SIS of alerts in respect of third-country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry into and stay on the territory of the Member States.
2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency on the operational management of large-scale IT systems in the area of freedom, security and justice, general data processing, the rights of the persons concerned and liability.

Article 3

Definitions

1. For the purposes of this Regulation, the following definitions shall apply:
 - (a) ‘alert’ means a set of data, including biometric identifiers as referred to in Article 22, entered in SIS allowing the competent authorities to identify a person with a view to taking specific action;
 - (b) ‘supplementary information’ means information not forming part of the alert data stored in SIS, but connected to SIS alerts, which is to be exchanged:
 - (1) in order to allow Member States to consult or inform each other when entering an alert;
 - (2) following a hit in order to allow the appropriate action to be taken;
 - (3) when the required action cannot be taken;
 - (4) when dealing with the quality of SIS data;
 - (5) when dealing with the compatibility and priority of alerts;
 - (6) when dealing with rights of access;
 - (c) ‘additional data’ means the data stored in SIS and connected with SIS alerts which are to be immediately available to the competent authorities where a

person in respect of whom data has been entered in SIS is located as a result of searches made therein;

- (d) ‘third-country national’ means any person who is not a citizen of the Union within the meaning of Article 20 of the TFEU, with the exception of persons who enjoy rights of free movement equivalent to those of Union citizens under agreements between the Union, or the Union and its Member States on the one hand, and third countries on the other hand;
- (e) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);
- (f) ‘an identifiable natural person’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (g) ‘processing of personal data’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (h) a ‘hit’ in SIS means:
 - (1) a search is conducted by a user,
 - (2) the search reveals an alert entered by another Member State in SIS,
 - (3) data concerning the alert in SIS matches the search data, and
 - (4) further actions are requested as a result of the hit
- (i) ‘issuing Member State’ means the Member State which entered the alert in SIS;
- (j) ‘executing Member State’ means the Member State which takes the required actions following a hit;
- (k) ‘end-users’ mean competent authorities directly searching CS-SIS, N.SIS or a technical copy thereof.
- (l) ‘return’ means return as defined in point 3 of Article 3 of Directive 2008/115/EC;
- (m) ‘entry ban’ means entry ban as defined in point 6 of Article 3 of Directive 2008/115/EC;
- (n) ‘dactylographic data’ means data on fingerprints and palm prints which due to their unique character of uniqueness and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

- (o) ‘serious crime’ means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002⁶⁸;
- (p) ‘terrorist offences’ means offences under national law referred to in Articles, 1-4 of Framework Decision 2002/475/JHA of 13 June 2002⁶⁹.

Article 4

Technical architecture and ways of operating SIS

1. SIS shall be composed of:
 - (a) a central system (Central SIS) composed of:
 - a technical support function (‘CS-SIS’) containing a database, the ‘SIS database’,
 - a uniform national interface (NI-SIS);
 - (b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS shall contain a data file (a ‘national copy’), containing a complete or partial copy of the SIS database as well as a backup N.SIS. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users;
 - (c) a communication infrastructure between CS-SIS and NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS data and the exchange of data between SIRENE Bureaux as referred to in Article 7(2).
2. SIS data shall be entered, updated, deleted and searched via the various N.SIS. A partial or a full national copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. The partial national copy shall contain at least the data listed in Article 20(2) (a)-(v) of this Regulation. It shall not be possible to search the data files of other Member States' N.SIS.
3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system. CS-SIS and the backup CS-SIS shall be located in the two technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011⁷⁰ (‘the Agency’). CS-SIS or backup CS-SIS may contain an additional copy of the SIS database and may be used simultaneously in active operation provided that each of them is capable to process all transactions related to SIS alerts.
4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. CS-SIS shall:

⁶⁸ Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.07.2002, p. 1).

⁶⁹ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

⁷⁰ Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

- (a) provide online update of the national copies;
- (b) ensure synchronisation of and consistency between the national copies and the SIS database;
- (c) provide the operation for initialisation and restoration of the national copies;
- (d) provide uninterrupted availability.

Article 5

Costs

1. The costs of operating, maintaining and further developing Central SIS and the Communication Infrastructure shall be borne by the general budget of the European Union.
2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).
3. The costs of setting up, operating, maintaining and further developing each N.SIS shall be borne by the Member State concerned.

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 6

National systems

Each Member State shall be responsible for setting up, operating, maintaining and further developing its N.SIS and connecting its N.SIS to NI-SIS.

Each Member State shall be responsible for ensuring the continuous operation of the N.SIS, its connection to NI-SIS and the uninterrupted availability of SIS data to the end-users.

Article 7

N.SIS Office and SIRENE Bureau

1. Each Member State shall designate an authority (the N.SIS Office), which shall have central responsibility for its N.SIS.

That authority shall be responsible for the smooth operation and security of the N.SIS, shall ensure the access of the competent authorities to the SIS and shall take the necessary measures to ensure compliance with the provisions of this Regulation. It shall be responsible for ensuring that all functionalities of SIS are appropriately made available to the end-users.

Each Member State shall transmit its alerts via its N.SIS Office.

2. Each Member State shall designate the authority which shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.

Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS. For those purposes they shall have access to data processed in SIS.

3. The Member States shall inform the Agency of their N.SIS II Office and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 36(8).

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and personal resources to ensure the continuous availability and exchange of supplementary information. In the event that the the Communication Infrastructure is unavailable, Member States may use other adequately secured technical means to exchange supplementary information.
2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 43 unless prior consent is obtained from the issuing Member State.
3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by replying to a request as soon as possible but not later than 12 hours after the receipt of the request.
4. Detailed rules for the exchange of supplementary information shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 55(2) in the form of a manual called the 'SIRENE Manual'.

Article 9

Technical and functional compliance

1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N-SIS with CS-SIS for the prompt and effective transmission of data. Those common standards, protocols and technical procedures shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).
2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy are, by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS database, and that a search in its national copy produces a result equivalent to that of a search in the SIS database. End-users shall receive the data required to perform their tasks, in particular all data required for the identification of the data subject and to take the required action.

Article 10

Security – Member States

1. Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;
 - (b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);

- (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
 - (d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
 - (e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
 - (f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);
 - (g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 50(1) without delay upon their request (personnel profiles);
 - (h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
 - (i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);
 - (j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control);
 - (k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring (self-auditing).
2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information, including securing the premises of the SIRENE Bureau.
 3. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing of SIS data by the authorities referred to in Article 29.

Article 11 *Confidentiality – Member States*

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

Article 12
Keeping of logs at national level

1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS , data integrity and security.
2. The logs shall show, in particular, the history of the alert, the date and time of the data processing activity, the type of data used to perform a search, a reference to the of type data transmitted and the name of both the competent authority and the person responsible for processing the data.
3. If the search is carried out with dactylographic data or facial image in accordance with Article 22 the logs shall show, in particular, the type of data used to perform a search, a reference to the type data transmitted and the name of both the competent authority and the person responsible for processing the data.
4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation.
5. Logs may be kept longer if they are required for monitoring procedures that are already under way.
6. The competent national authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to these logs for the purpose of fulfilling their duties.

Article 13
Self-monitoring

Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the national supervisory authority.

Article 14
Staff training

Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data-security, data-protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties.

CHAPTER III

RESPONSIBILITIES OF THE AGENCY

Article 15

Operational management

1. The Agency shall be responsible for the operational management of Central SIS. The Agency shall ensure, in cooperation with the Member States, ensure that at all times the best available technology, using a cost-benefit analysis, is used for Central SIS.
2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure.
 - (a) supervision;
 - (b) security;
 - (c) the coordination of relations between the Member States and the provider;
3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:
 - (a) tasks relating to implementation of the budget;
 - (b) acquisition and renewal;
 - (c) contractual matters.
4. The Agency shall also be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:
 - (a) the coordination and management of testing;
 - (b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the communication infrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.
5. The Agency shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States. The Agency shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. This mechanism, procedures and interpretation of data quality compliance shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).
6. Operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, seven days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks also include testing activities ensuring that Central SIS and the national systems operate in accordance with the technical and functional requirements in accordance with Article 9 of this Regulation.

Article 16
Security

1. The Agency shall adopt the necessary measures, including of a security plan a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;
 - (b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);
 - (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
 - (d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
 - (e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
 - (f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation by means of individual and unique user identities and confidential access modes only (data access control);
 - (g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 51 without delay upon its request (personnel profiles);
 - (h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
 - (i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom the data were input (input control);
 - (j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control);
 - (k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).
2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information through the Communication Infrastructure.

Article 17
Confidentiality – Agency

1. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of

confidentiality of comparable standards to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.

2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the Communication Infrastructure.

Article 18

Keeping of logs at central level

1. The Agency shall ensure that every access to and all exchanges of personal data within CS-SIS are logged for the purposes mentioned in Article 12(1).
2. The logs shall show, in particular, the history of the alerts, the date and time of the data transmitted, the type of data used to perform searches, the reference to the type of data transmitted and the name of the competent authority responsible for processing the data.
3. If the search is carried out with dactylographic data or facial image in accordance with Article 22 and 28 the logs shall show, in particular, the type of data used to perform a search, a reference to the type data transmitted and the name of both the competent authority and the person responsible for processing the data.
4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The logs which include the history of alerts shall be erased after one to three years after deletion of the alerts.
5. Logs may be kept longer if they are required for monitoring procedures that are already underway.
6. The competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to those logs for the purpose of fulfilling their tasks.

CHAPTER IV

INFORMATION TO THE PUBLIC

Article 19

SIS information campaigns

The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall regularly carry out campaigns informing the public about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens about SIS generally.

CHAPTER V

ALERTS ISSUED IN RESPECT OF THIRD-COUNTRY NATIONALS FOR THE PURPOSE OF REFUSING ENTRY AND STAY

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Article 24.
2. The information on persons in relation to whom an alert has been issued shall only contain the following data:
 - (a) surname(s);
 - (b) forename(s);
 - (c) name(s) at birth;
 - (d) previously used names and aliases;
 - (e) any specific, objective, physical characteristics not subject to change;
 - (f) place of birth;
 - (g) date of birth;
 - (h) sex;
 - (i) nationality/nationalities;
 - (j) whether the person concerned is armed, violent, has escaped or is involved in an activity as referred to in Articles 1, 2 , 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism;
 - (k) reason for the alert;
 - (l) authority issuing the alert;
 - (m) a reference to the decision giving rise to the alert;
 - (n) action to be taken;
 - (o) link(s) to other alerts issued in SIS pursuant to Article 38;
 - (p) whether the person concerned is a family member of an EU citizen or other person who enjoys rights of free movement as referred to in Article 25;
 - (q) whether the decision on refusal of entry is based on:
 - a previous conviction as referred to in Article 24(2)(a);
 - a serious security threat as referred to in Article 24(2)(b);
 - an entry ban as referred to in Article 24(3); or
 - a restrictive measure as referred to in Article 27;
 - (r) type of offence (for alerts issued pursuant to Article 24(2) of this Regulation);

- (s) the category of the person's identification document;
 - (t) the country of issue of the person's identification document;
 - (u) the number(s) of the person's identification document;
 - (v) the date of issue of the person's identification document;
 - (w) photographs and facial images;
 - (x) dactylographic data;
 - (y) a colour copy of the identification document.
3. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).
 4. The technical rules necessary for searching the data referred to in paragraph 2 shall be laid down and developed in accordance with the examination procedure referred to in Article 55(2). These technical rules shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 36 and they shall be based upon common standards laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

Article 21

Proportionality

1. Before issuing an alert and when extending the validity period of an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant the entry of an alert in SIS.
2. In the application of Article 24(2) Member States shall, in all circumstances, create such an alert in relation to third country nationals if the offence falls under Articles 1 – 4 of Council Framework Decision 2002/475/JHA on combating terrorism⁷¹.

Article 22

Specific rules for entering photographs, facial images and dactylographic data

1. Data referred to in Article 20(2)(w) and (x) shall only be entered into SIS following a quality check to ascertain the fulfilment of a minimum data quality standard.
2. Quality standards shall be established for the storage of the data referred to under paragraph 1. The specification of these standards shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 55(2).

⁷¹ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

Article 23

Requirement for an alert to be entered

1. An alert may not be entered without the data referred to in Article 20(2)(a), (g),(k),(m),(n) and (q). Where an alert is based upon a decision taken under Article 24 (2) the data referred to in Article 20(2)(r) shall also be entered.
2. Where available, all other data listed in Article 20(2) shall also be entered.

Article 24

Conditions for issuing alerts on refusal of entry and stay

1. Data on third-country nationals in respect of whom an alert has been issued for the purposes of refusing entry and stay shall be entered in SIS on the basis of a national alert resulting from a decision taken by the competent administrative or judicial authorities in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment. Appeals against those decisions shall be made in accordance with national law.
2. An alert shall be entered where the decision referred to in paragraph 1 is based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a Member State may pose. This situation shall arise in particular in the case of:
 - (a) a third-country national who has been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year;
 - (b) a third-country national in respect of whom there are serious grounds for believing that he has committed a serious crime or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State.
3. An alert shall be entered where the decision referred to in paragraph 1 is an entry ban issued in accordance with procedures respecting Directive 2008/115/EC. The issuing Member State shall ensure that the alert takes effect in SIS at the point of return of the third-country national concerned. The confirmation of return shall be communicated to the issuing Member State in accordance with Article 6 of Regulation (EU) 2018/xxx [Return Regulation].

Article 25

Conditions for entering alerts on third-country nationals who are beneficiaries of the right of free movement within the Union

1. An alert concerning a third-country national who is a beneficiary of the right of free movement within the Union, within the meaning of Directive 2004/38/EC of the European Parliament and of the Council⁷² shall be entered in accordance with the measures adopted to implement that Directive.
2. Where there is a hit on an alert pursuant to Article 24 concerning a third-country national who is a beneficiary of the right of free movement within the Union, the Member State executing the alert shall immediately consult the issuing Member

⁷² OJ L 158, 30.4.2004, p.77.

State, through the exchange of supplementary information, in order to decide without delay on the action to be taken.

Article 26
Consultation procedure

1. Where a Member State considers granting a residence permit or other authorisation offering a right to stay to a third-country national who is the subject of an alert for refusal of entry and stay entered by another Member State, it shall first consult the issuing Member State through the exchange of supplementary information and shall take account of the interests of that Member State. The issuing Member State shall provide a definite reply within seven days. Where the Member State considering granting a permit or other authorisation offering a right to stay decides to grant it, the alert for refusal of entry and stay shall be deleted.
2. Where a Member State considers entering an alert for refusal of entry and stay concerning a third-country national who is the holder of a valid residence permit or other authorisation offering a right to stay issued by another Member State, it shall first consult the Member State that issued the permit through the exchange of supplementary information and shall take account of the interests of that Member State. The Member State that issued the permit shall provide a definite reply within seven days. If the Member State that issued the permit decides to maintain it, the alert for refusal of entry and stay shall not be entered.
3. In the event of a hit on an alert for refusal of entry and stay concerning a third-country national who is the holder of a valid residence permit or other authorisation offering a right to stay, the executing Member State shall consult immediately the Member State that issued the residence permit and the Member State that entered the alert, respectively, via the exchange of supplementary information in order to decide without delay if the action may be taken. If it is decided to maintain the residence permit, the alert shall be deleted.
4. Member States shall provide on an annual basis statistics to the Agency about the consultations carried out in accordance with paragraphs 1 to 3.

Article 27
Conditions for issuing alerts on third-country nationals subject to restrictive measures

1. Alerts relating to third-country nationals, who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with legal acts adopted by the Council, including measures implementing a travel ban issued by the Security Council of the United Nations, shall insofar as data-quality requirements are satisfied, be entered in SIS for the purpose of refusing entry and stay.
2. The Member State responsible for entering, updating and deleting these alerts on behalf of all Member States shall be designated at the moment of the adoption of the relevant measure taken in accordance with Article 29 of the Treaty on European Union. The procedure for designating the Member State responsible shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

CHAPTER VI

SEARCH WITH BIOMETRIC DATA

Article 28

Specific rules for verification or search with photographs, facial images and dactylographic data

1. Photographs, facial images and dactylographic data shall be retrieved from SIS to verify the identity of a person who has been located as a result of an alphanumeric search made in SIS.
2. Dactylographic data may also be used to identify a person. Dactylographic data stored in SIS shall be used for identification purposes if the identity of the person cannot be ascertained by other means.
3. Dactylographic data stored in SIS in relation to alerts issued under Article 24 may also be searched with complete or incomplete sets of fingerprints or palm prints discovered at the scenes of crimes under investigation and where it can be established to a high degree of probability that they belong to the perpetrator of the offence provided that the competent authorities are unable to establish the identity of the person by using any other national, European or international database.
4. As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. Identification based on photographs or facial images shall only be used in the context of regular border crossing points where self-service systems and automated border control systems are in use.

CHAPTER VII

RIGHT TO ACCESS AND RETENTION OF ALERTS

Article 29

Authorities having a right to access alerts

1. Access to data entered in SIS and the right to search such data directly or in a copy of SIS data shall be reserved to the authorities responsible for the identification of third-country nationals for the purposes of:
 - (a) border control, in accordance with 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);
 - (b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;
 - (c) other law enforcement activities carried out for the prevention, detection and investigation of criminal offences within the Member State concerned;
 - (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals;

- (e) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EU) No 810/2009 of the European Parliament and of the Council.⁷³
- 2. For the purposes of Article 24(2) and (3) and Article 27 the right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.
- 3. The right to access data concerning documents relating to persons entered in accordance with Article 38(2)(j) and (k) of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters] and the right to search such data may also be exercised by the authorities referred to in paragraph 1(d). Access to data by these authorities shall be governed by the law of each Member State.
- 4. The authorities referred to in this Article shall be included in the list referred to in Article 36(8).

Article 30
Access to SIS data by Europol

- 1. The European Union Agency for Law Enforcement Cooperation (Europol) shall have within its mandate, have the right to access and search data entered into SIS.
- 2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State via the channels defined by Regulation (EU) 2016/794.
- 3. The use of information obtained from a search in the SIS is subject to the consent of the Member State concerned. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the Member State concerned.
- 4. Europol may request further information from the Member State concerned in accordance with the provisions of Regulation (EU) 2016/794.
- 5. Europol shall:
 - (a) without prejudice to paragraphs 3, 4 and 6, not connect parts of SIS nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS;
 - (b) limit access to data entered in SIS to specifically authorised staff of Europol;
 - (c) adopt and apply measures provided for in Articles 10 and 11;
 - (d) allow the European Data Protection Supervisor to review the activities of Europol in the exercise of its right to access and search data entered in SIS.

⁷³

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.
7. Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end. Europol shall report any such extensions to the European Data Protection Supervisor.
8. Europol may receive and process supplementary information on corresponding SIS alerts provided that the data processing rules referred to in paragraphs (2)-(7) are applied as appropriate.
9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol should keep logs of every access to and search in SIS. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.

Article 31

Access to SIS data by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams

1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall, within their mandate, have the right to access and search data entered in SIS within their mandate.
2. Members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 32(2).
3. Where a search by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams reveals the existence of an alert in SIS, the issuing Member State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.
4. Every instance of access and every search made by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be registered.

5. Access to data entered in SIS shall be limited to a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams and shall not be extended to any other team member.
6. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied.

Article 32

Access to SIS data by the European Border and Coast Guard Agency

1. The European Border and Coast Guard Agency shall, for the purpose of analysing the threats that may affect the functioning or security of the external borders, have the right to access and search data entered in SIS, in accordance with Articles 24 and 27.
2. For the purposes of Article 31(2) and paragraphs 1 of this Article the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.
3. Where a search by the European Border and Coast Guard Agency reveals the existence of an alert in SIS, it shall inform the issuing Member State.
4. The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and verify data entered in SIS, in accordance with Articles 24 and 27.
5. Where a verification by the European Border and Coast Guard Agency for the purposes of paragraph 2 reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.
6. Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection and the liability for any unauthorised or incorrect processing of such data by the European Border and Coast Guard Agency.
7. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 12 and every use made of data accessed by the European Border and Coast Guard Agency shall be registered.
8. Except where necessary to perform the tasks for the purposes of the Regulation establishing a European Travel Information and Authorisation System (ETIAS) no parts of SIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency nor shall the data contained in SIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.
9. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied.

Article 33
Scope of access

End-users, including Europol, and the European Border and Coast Guard Agency, may only access data which they require for the performance of their tasks.

Article 34
Retention period of alerts

1. Alerts entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.
2. A Member State issuing an alert shall, within five years of its entry into SIS, review the need to retain it.
3. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.
4. In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall notify the authority which created the alert to bring this issue to the attention of the authority. The authority shall have 30 calendar days from the receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the 30-day period expires without such a reply the alert shall be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.
5. Within the review period, the Member State issuing the alert may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. In such a case, paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.
6. Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the Member State issuing the alert has informed CS-SIS about the extension of the alert to CS-SIS pursuant to paragraph 5. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.
7. Member States shall keep statistics about the number of alerts or which the retention period has been extended in accordance with paragraph 5.

Article 35
Deletion of alerts

1. Alerts on refusal of entry and stay pursuant to Article 24 shall be deleted when the decision on which the alert was entered has been withdrawn by the competent authority, where applicable following the consultation procedure referred to in Article 26.
2. Alerts relating to third-country nationals who are the subject of a restrictive measure as referred to in Article 27 shall be deleted when the measure implementing the travel ban has been terminated, suspended or annulled.

3. Alerts issued in respect of a person who has acquired citizenship of any State whose nationals are beneficiaries of the right of free movement within the Union shall be deleted as soon as the issuing Member State becomes aware, or is informed pursuant to Article 38 that the person in question has acquired such citizenship.

CHAPTER VIII

GENERAL DATA PROCESSING RULES

Article 36

Processing of SIS data

1. The Member States may process the data referred to in Article 20 for the purposes of refusing entry into and stay in their territories.
2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 29 to carry out a direct search. The provisions of this Regulation shall apply to such copies. A Member State shall not copy alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files.
3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in the event of an emergency until the emergency comes to an end.

Notwithstanding the first subparagraph, technical copies which lead to off-line databases to be used by visa issuing authorities shall not be permitted, except for copies made to be used only in an emergency following the unavailability of the network for more than 24 hours.

Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of Article 10, are applied in respect of those copies.

4. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 29 and to duly authorised staff.
5. Any processing of information contained in SIS for purposes other than those for which it was entered in SIS has to be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the Member State issuing the alert shall be obtained for this purpose.
6. Data concerning documents related to persons entered under Article 38(2)(j) and (k) of Regulation (EU) 2018/xxx may be used by the authorities referred to in Article 29(1)(d) in accordance with the laws of each Member State.
7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State.
8. Each Member State shall send to the Agency a list of its competent authorities which are authorised to search directly the data contained in SIS pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each

authority, which data it may search and for what purposes. The Agency shall ensure the annual publication of the list in the *Official Journal of the European Union*.

9. In so far as Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS.

Article 37

SIS data and national files

1. Article 36(2) shall not prejudice the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.
2. Article 36(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS by that Member State.

Article 38

Information in case of non-execution of alert

If a requested action cannot be performed, the requested Member State shall immediately inform the Member State issuing the alert.

Article 39

Quality of the data processed in SIS

1. A Member State issuing an alert shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.
2. Only the Member State issuing an alert shall be authorised to modify, add to, correct, update or delete data which it has entered.
3. Where a Member State other than that which issued an alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than 10 days after the said evidence has come to its attention. The issuing Member State shall check the communication and, if necessary, correct or delete the item in question without delay.
4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the national supervisory authorities concerned for a decision.
5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 42.
6. Where a person is already the subject of an alert in SIS, a Member State which enters a further alert shall reach agreement on the entry of the alert with the Member State which entered the first alert. The agreement shall be reached on the basis of the exchange of supplementary information.

Article 40
Security incidents

1. Any event that has or may have an impact on the security of SIS and may cause damage or loss to SIS data shall be considered to be a security incident, especially where access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.
2. Security incidents shall be managed to ensure a quick, effective and proper response.
3. Member States shall notify the Commission, the Agency and the European Data Protection Supervisor of security incidents. The Agency shall notify the Commission and the European data Protection Supervisor of security incidents.
4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States, shall be provided to the Member States and reported in compliance with the incident management plan provided by the Agency.

Article 41
Distinguishing between persons with similar characteristics

Where it becomes apparent, when a new alert is entered, that there is already a person in SIS with the same identity description element, the following procedure shall apply:

- (a) the SIRENE Bureau shall contact the requesting authority to clarify whether or not the alert is on the same person;
- (b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 39(6). Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.

Article 42
Additional data for the purpose of dealing with misused identities

1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification.
2. Data relating to a person whose identity has been misused shall be used only for the following purposes:
 - (a) to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert;
 - (b) to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.
3. For the purpose of this Article, only the following personal data may be entered and further processed in SIS:
 - (a) surname(s)

- (b) forename(s),
 - (c) name(s) at birth
 - (d) previously used names and any aliases possibly entered separately;
 - (e) any specific objective and physical characteristic not subject to change;
 - (f) place of birth
 - (g) date of birth;
 - (h) sex;
 - (i) facial images;
 - (j) fingerprints;
 - (k) nationality(ies);
 - (l) the category of the person's identity document
 - (m) the country of issue of the person's identity document
 - (n) the number(s) of the person's identity document
 - (o) the date of issue of a person's identity document
 - (p) address of the victim
 - (q) victim's father's name
 - (r) victim's mother's name
4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established by means of implementing measures laid down and developed in accordance with the examination procedure referred to in Article 55(2).
 5. The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.
 6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.

Article 43
Links between alerts

1. A Member State may create a link between alerts it enters in SIS. The effect of such a link shall be to establish a relationship between two or more alerts.
2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention period of each of the linked alerts.
3. The creation of a link shall not affect the rights of access provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.
4. A Member State shall create a link between alerts when there is an operational need.
5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it

may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.

6. The technical rules for linking alerts shall be laid down and developed in accordance with the examination procedure defined in Article 55(2).

Article 44

Purpose and retention period of supplementary information

1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.
2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.
3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.

Article 45

Transfer of personal data to third parties

Data processed in SIS and the related supplementary information pursuant to this Regulation shall not be transferred or made available to third countries or to international organisations.

CHAPTER IX

DATA PROTECTION

Article 46

Applicable legislation

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency under this Regulation.
2. Regulation 2016/679 shall apply to the processing of personal data by the authorities referred to in Article 29 of this Regulation provided that national provisions transposing Directive (EU) 2016/680 do not apply.
3. For processing of data by competent national authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties including the safeguarding against the prevention of threat to public security national provisions transposing Directive (EU) 2016/680 shall apply.

Article 47

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

1. The right of data subjects to have access to data relating to them entered in SIS and to have such data rectified or erased shall be exercised in accordance with the law of the Member State before which they invoke that right.
2. If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what means.
3. A Member State other than that which has issued an alert may communicate information concerning such data only if it first gives the Member State issuing the alert an opportunity to state its position. This shall be done through the exchange of supplementary information.
4. A Member State shall take a decision not to communicate information to the data subject, in whole or in part, in accordance with national law, 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 natural person 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;
 - (e) protect the rights and freedoms of others.
5. The person concerned shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides.
6. The person concerned shall be informed about the follow-up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than three months from the date on which he applies for rectification or erasure or sooner if national law so provides.

Article 48

Right of information

1. Third-country nationals who are the subject of an alert issued in accordance with this Regulation shall be informed in accordance with Articles 10 and 11 of Directive 95/46/EC. This information shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert, as referred to in Article 24(1).
2. This information shall not be provided:
 - (f) where:
 - i) the personal data have not been obtained from the third-country national in question;and

- ii) the provision of the information proves impossible or would involve a disproportionate effort;
- (g) where the third country national in question already has the information;
- (h) where national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

Article 49 *Remedies*

1. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, rectify, delete or erase information or to obtain compensation in connection with an alert relating to him.
2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 53.
3. In order to gain a consistent overview of the functioning of remedies the national supervisory authorities shall be invited to develop a standard statistical system for reporting annually on:
 - (a) the number of subject access requests submitted to the data controller and the number of cases where access to the data was granted;
 - (b) the number of subject access requests submitted to the national 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 the erasure of unlawfully stored data to the data controller and the number of cases where the data were corrected or deleted;
 - (d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the national supervisory authority;
 - (e) the number of cases which are heard before the courts;
 - (f) the number of cases where the court ruled in favour of the applicant in any aspect of the case;
 - (g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the alert-issuing Member State.

The reports from the national supervisory authorities shall be forwarded to the cooperation mechanism set out in Article 52.

Article 50 *Supervision of N.SIS*

1. Each Member State shall ensure that the independent national supervisory authorit(ies) designated in each Member State and endowed with the powers referred to in Chapter VI of Directive (EU)2016/680 or Chapter VI of Regulation (EU) 2016/679 monitor independently the lawfulness of the processing of SIS personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information.

2. The national supervisory authority shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the national supervisory authority(ies), or the national supervisory authority(ies) shall directly order the audit from an independent data protection auditor. The national supervisory authority shall at all times retain control over and undertake the responsibilities of the independent auditor.
3. Member States shall ensure that their national supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

Article 51
Supervision of the Agency

1. The European Data Protection Supervisor shall ensure that the personal data processing activities of the Agency are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.
2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Article 52
Cooperation between national supervisory authorities and the European Data Protection Supervisor

1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of SIS.
2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of this Regulation and other applicable legal acts of the Union, study problems that are revealed through the exercise of independent supervision or through the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.
3. For the purposes laid down in paragraph 2, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year as part of the European Data Protection Board established by Regulation (EU) 2016/679. The costs and servicing of these meetings shall be borne by the Board established by Regulation (EU) 2016/679. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.
4. A joint report of activities as regards coordinated supervision shall be sent by the Board established by Regulation (EU) 2016/679 to the European Parliament, the Council, and the Commission every two years.

CHAPTER X

LIABILITY

Article 53

Liability

1. Each Member State shall be liable for any damage caused to a person through the use of N.SIS. This shall also apply to damage caused by the issuing Member State, where the latter entered factually inaccurate data or stored data unlawfully.
2. Where the Member State against which an action is brought is not the Member State issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the use of data by the Member State requesting reimbursement infringes this Regulation.
3. Where any failure by a Member State to comply with its obligations under this Regulation causes damage to SIS, that Member State shall be held liable for the damage, unless and in so far as the Agency or another Member States participating in SIS failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

CHAPTER XI

FINAL PROVISIONS

Article 54

Monitoring and statistics

1. The Agency shall ensure that procedures are in place to monitor the functioning of SIS against objectives, relating to output, cost-effectiveness, security and quality of service.
2. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in Central SIS.
3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, the annual 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 in total and for each Member State, including statistics on the consultation procedure referred to in Article 26. The statistics produced shall not contain any personal data. The annual statistical report shall be published.
4. Member States as well as Europol and the European Border and Coast Guard Agency shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraphs 7 and 8.
5. The Agency shall provide the Member States, the Commission, Europol and the European Border and Coast Guard Agency with any statistical reports that it

produces. In order to monitor the implementation of legal acts of the Union, the Commission shall be able to request the Agency to provide additional specific statistical reports, either regular or ad-hoc, on the performance or use of SIS and SIRENE communication.

6. For the purpose of paragraphs 3 to 5 of this Article and Article 15(5), the Agency shall establish, implement and host a central repository in its technical sites containing the data referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals and shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. The Agency shall grant access to Member States, the Commission, Europol and the European Border and Coast Guard Agency to the central repository by means of secured access through the Communication Infrastructure with control of access and specific user profiles solely for the purpose of reporting and statistics.

Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be laid down and developed by means of implementing measures adopted in accordance with the examination procedure referred to in Article 55(2).

7. Two years after SIS is brought into operation and every two years thereafter, the Agency shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.
8. Three years after SIS is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Article 55 *Committee procedure*

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 56 *Amendments to Regulation (EU) 515/2014*

Regulation (EU) 515/2014⁷⁴ is amended as follows:

In Article 6, the following paragraph 6 is inserted:

⁷⁴ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa (OJ L 150, 20.5.2014, p. 143).

“6. During the development phase Member States shall receive an additional allocation of 36,8 million EUR to be distributed via a lump sum to their basic allocation and shall entirely devote this funding to SIS national systems to ensure their quick and effective upgrading in line with the implementation of Central SIS as required in Regulation (EU) 2018/...^{*} and in Regulation (EU) 2018/...^{**}

^{*}Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police and judicial cooperation for criminal matters and in Regulation (OJ)....

^{**}Regulation (EU) 2018/...on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and in Regulation (OJ ...)”

Article 57

Repeal

Regulation (EC) No 1987/2006 on the establishment, operation and use of the second generation Schengen Information System;

Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure.⁷⁵

Article 25 of the Convention implementing the Schengen Agreement.⁷⁶

Article 58

Entry into force and applicability

1. This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.
2. It shall apply from the date fixed by the Commission after:
 - (a) the necessary implementing measures have been adopted;
 - (b) Member States have notified the Commission about that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation;
 - (c) The Agency has notified the Commission about the completion of all testing activities with regard CS-SIS and the interaction between CS-SIS and N.SIS.
3. This Regulation shall be binding in its entirety and directly applicable to Member States in accordance with the Treaty on the Functioning of the European Union.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

⁷⁵ Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p.31).

⁷⁶ OJ L 239, 22.9.2000, p. 19.

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

- 1.1. Title of the proposal/initiative
- 1.2. Policy area(s) concerned in the ABM/ABB structure
- 1.3. Nature of the proposal/initiative
- 1.4. Objective(s)
- 1.5. Grounds for the proposal/initiative
- 1.6. Duration and financial impact
- 1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

- 2.1. Monitoring and reporting rules
- 2.2. Management and control system
- 2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

- 3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected
- 3.2. Estimated impact on expenditure
 - 3.2.1. *Summary of estimated impact on expenditure*
 - 3.2.2. *Estimated impact on operational appropriations*
 - 3.2.3. *Estimated impact on appropriations of an administrative nature*
 - 3.2.4. *Compatibility with the current multiannual financial framework*
 - 3.2.5. *Third-party contributions*
- 3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and repealing Regulation (EC) No 1987/2006.

1.2. Policy area(s) concerned in the ABM/ABB structure⁷⁷

Policy area: Migration and Home Affairs (Title 18)

1.3. Nature of the proposal/initiative

- ☐ The proposal/initiative relates to **a new action**
- ☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**⁷⁸
- ☒ The proposal/initiative relates to **the extension of an existing action**
- ☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objective(s)

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

Objective – "Towards a new policy on migration"

The necessity to review the legal basis of SIS in order to address new security and migration challenges has been emphasised by the Commission on a number of occasions. In the "European Agenda on Migration"⁷⁹, for example, the Commission stated that managing the borders more efficiently implies making better use of the opportunities provided by IT systems and technologies. In the "European Agenda on Security"⁸⁰ the Commission announced its intention to evaluate SIS in 2015-2016 and to look into possibilities to assist the Member States in implementing travel bans set at national level. In the "EU Action plan against migrant smuggling"⁸¹, the Commission stated that it was considering making it obligatory for Member States' authorities to introduce all entry bans in SIS in order to enable their EU-wide enforcement. Moreover, the Commission also stated that it would explore the possibility and proportionality of introducing return decisions issued by the Member States' authorities to see if an apprehended irregular migrant is subject to a return decision issued by another Member State. Finally, in the "Smarter and Stronger Information Systems for Borders and Security"⁸², the Commission highlighted that it was exploring possible additional functionalities in SIS with related proposals to revise the legal basis of the system.

⁷⁷ ABM: activity-based management; ABB: activity-based budgeting.

⁷⁸ As referred to in Article 54(2)(a) or (b) of the Financial Regulation.

⁷⁹ COM(2015) 240 final.

⁸⁰ COM(2015) 185 final.

⁸¹ COM(2015) 285 final.

⁸² COM(2016) 205 final.

As a result of the overall evaluation of the system and fully in line with the Commission's multiannual objectives, stated in the above-mentioned communications and the Strategic Plan 2016-2020 of DG Migration and Home Affairs⁸³, this proposal aims to reform the structure, operation and use of the Schengen Information System in the field of border checks.

1.4.2. *Specific objective(s) and ABM/ABB activity(ies) concerned*

Specific objective No

DG Migration and Home Affairs Management Plan 2017 - Specific objective No 1.2:
Effective border management – save lives and secure EU external borders

ABM/ABB activity(ies) concerned

Chapter 18 02 – Internal Security

⁸³ Ares(2016)2231546 – 12/05/2016.

1.4.3. *Expected result(s) and impact*

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

The main objectives of the policy are:

1). To contribute to a high level of security within the area of freedom, security and justice of the EU;

2) To reinforce the effectiveness and efficiency of border controls;

The overall evaluation of SIS, carried out by DG HOME in 2015-2016, recommended technical enhancements of the system and harmonisation of national procedures in the field of managing refusals of entry and stay. For example, the current SIS II Regulation only allows and does not require Member States to issue alerts for refusal of entry and stay in the system. Some Member States systematically enter all entry bans in SIS, whereas others do not. Therefore, the current proposal will contribute to achieving a greater level of harmonisation in this area by making it obligatory to enter all entry bans in SIS, and define common rules on entering the alerts in the system and specify the underlying reason for the alert.

The new proposal introduces measures which address end-users' operational and technical needs. In particular, new data fields for existing alerts will enable border guards to have all the necessary information to perform their tasks effectively. Furthermore, the proposal specifically emphasises the importance of uninterrupted availability of SIS, as downtimes can significantly impact the ability to carry out external border controls. Hence, this proposal will have a highly positive effect upon the effectiveness of border controls.

Once adopted and implemented, these proposals will also increase business continuity – Member States will be obliged to have a full or partial national copy and a back-up of this. This will enable the system to remain fully functional and operational for officers on the ground.

1.4.4. *Indicators of results and impact*

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

During the upgrading of the system

After the approval of the draft proposal and the adoption of the technical specifications, SIS will be upgraded in order to better harmonise national procedures for the use of the system, extend the scope of the system by enhancing the levels of information available to end-users in order to better inform officers carrying out checks, and introduce technical changes to improve security and help reduce administrative burdens. eu-LISA will coordinate the project management of upgrading the system. eu-LISA will establish a project management structure and provide a detailed timeline with milestones for implementing the proposed changes which will allow the Commission to closely monitor the implementation of the proposal.

Specific objective – Entry into operations of the updated functionalities of SIS in 2020.

Indicator – successful completion of comprehensive pre-launch testing of the revised system.

Once the system is operational

Once the system is operational, eu-LISA will ensure that procedures are in place to monitor the functioning of SIS against objectives, relating to output, cost-effectiveness, security and quality of service. Two years after SIS was brought into operations and every two years thereafter, eu-LISA is obliged to submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States. Furthermore, eu-LISA produces daily, monthly and annual statistics showing the number of logs per category of alert, the annual number of hits achieved per category of alert, how many times SIS was searched and how many times the system was accessed for the purpose of entering, updating or deleting an alert in total and for each Member State.

Three years after SIS is brought into operation and every four years thereafter, the Commission produces an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. This overall evaluation includes an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. The Commission sends the evaluation to the European Parliament and the Council.

1.5. Grounds for the proposal/initiative

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

1. Contribute to the maintenance of a high level of security within the area of freedom, security and justice of the EU;
2. Reinforce the fight against international criminality, terrorism and other security threats;
3. Extend the scope of SIS by introducing new elements to alerts for refusal of entry and stay;
4. Enhance the effectiveness of border controls;
5. Increase the efficiency of the work of border guards and the immigration authorities;
6. Achieve a greater level of effectiveness and harmonisation of the national procedures and ensure the enforceability of entry bans across the Schengen area;
7. Contribute to combating irregular migration.

1.5.2. Added value of EU involvement

SIS is the main security database in Europe. In the absence of internal border controls, the effective combatting of crime and terrorism gained a European dimension. Hence, SIS is indispensable when it comes to supporting external border controls and checks on irregular migrants found on the national territory. The objectives of this proposal pertain to technical improvements to enhance the efficiency and effectiveness of the system and to harmonise its use across participating Member States. The transnational nature of these aims, along with the challenges in ensuring effective information exchange to counter ever-diversifying threats, mean that the EU is in the best position to propose solutions to these problems. The objectives of enhancing the efficiency and harmonised use of SIS,

namely, the increase in the volume, the quality and the speed of the information exchange via a centralised large-scale information system managed by a regulatory agency (eu-LISA) cannot be achieved by Member States alone and require intervention at the EU level. If the present issues are not addressed, SIS will continue to operate in line with the rules applicable at present, thereby missing opportunities for maximising efficiency and EU added value identified through evaluation of SIS and its use by Member States.

In 2015 alone, national authorities queried SIS nearly 2.9 billion times and exchanged over 1.8 million pieces of supplementary information - a clear demonstration of the system's vital contribution to external border controls. This high level of information exchange between Member States would not have been reached through decentralised solutions, and it would have been impossible to achieve these results at national level. Furthermore, SIS has proved to be the most effective information exchange tool for counter-terrorism purposes and it provides EU added value as it allows the national security services to cooperate in a rapid, confidential and efficient manner. The new proposals will further facilitate the exchange of information and cooperation between the border control authorities of the EU Member States. Moreover, within their competences, Europol and the European Border and Coast Guard will be granted full access to the system as a clear sign of the added value of EU involvement.

1.5.3. *Lessons learned from similar experiences in the past*

The main lessons learned from the development of the second generation Schengen Information System were:

1. The development phase should commence only after the technical and operational requirements are fully defined. Development can only take place once the underlying legal instruments, setting out its purpose, scope, functions and technical details have been definitively adopted.

2. The Commission conducted (and continues to conduct) frequent consultations with the relevant stakeholders, including delegates to the SISVIS Committee under the Comitology procedure. This Committee includes the Member States' representatives on both operational SIRENE matters (cross-border cooperation in relation to SIS) and technical matters in the development and maintenance of SIS and the related SIRENE application. The changes proposed by this Regulation were discussed in a transparent and comprehensive way in dedicated meetings and workshops. Furthermore, internally, the Commission set up an Inter-service Steering Group encompassing the Secretariat-General and the Directorates-General for Migration and Home Affairs, Justice and Consumers, Human Resources and Security, and Informatics. This steering group monitored the evaluation process and provided guidance as needed.

3. The Commission also sought external expertise via three studies, the findings of which have been incorporated in the developments of this proposal:

- SIS Technical Assessment (Kurt Salmon) – the assessment identified key issues pertaining to SIS and future needs that should be considered; it identified concerns with regards to maximising business continuity and ensuring that the overall architecture can adapt to increasing capacity requirements.

- ICT Impact Assessment of Possible Improvements to the SIS II Architecture (Kurt Salmon) – the study assessed the current costs of operating SIS at national level and

evaluated three possible technical scenarios for the improvement of the system. All scenarios include a set of technical proposals focusing on improvements to the central system and overall architecture;

-Study on the feasibility and implications of setting up within the framework of the Schengen Information System an EU-wide system for exchanging data on and monitoring compliance with return decisions (PwC)- this study assesses the feasibility and the technical and operational implications of the proposed changes to SIS with the purpose of enhancing its use for the return of irregular migrants and for preventing their re-entry.

1.5.4. *Compatibility and possible synergy with other appropriate instruments*

This proposal should be seen as the implementation of the actions contained in the Communication of 6 April 2016 on "Stronger and Smarter Information Systems for Borders and Security"⁸⁴ which highlights the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the area of law enforcement, counter-terrorism and border management.

Moreover, the proposal is consistent with a number of Union policies in this area:

- a) Internal security in regards to the role of SIS for preventing the entry of third-country nationals posing a security threat;
- b) Data protection insofar as this proposal must ensure the protection of fundamental rights to respect for the private life of individuals whose personal data is processed in SIS.

The proposal is also compatible with existing European Union legislation, namely:

- a) An effective EU return policy in order to contribute to and enhance the EU system to detect and prevent the re-entry of third-country nationals following their return. This would contribute to the reduction of incentives to irregularly migrate to the EU, which is one of the main objectives of the European Agenda on Migration⁸⁵.b) **European Border and Coast Guard**⁸⁶: with regards the possibility for the Agency staff conducting risk analyses, as well as European Border and Coast Guard Teams, teams of staff involved in return-related tasks and members of the migration management support teams to, within their mandate, have the right to access and search data entered in SIS;
- c) **External border controls**, insofar as this Regulation assists individual Member States in controlling their portion of the EU's external borders and in building trust in the effectiveness of the EU system of border management;
- d) Europol insofar as this proposal grants Europol additional rights to access and search data entered in SIS within its mandate

The proposal is also compatible with future European Union legislation, namely:

⁸⁴ COM(2016) 205 final.

⁸⁵ COM(2015) 240 final.

⁸⁶ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251 of 16.9.2016, p. 1).

- a) **Entry/Exit System**⁸⁷ which proposes a combination of fingerprint and facial image as biometric identifiers for the operation of the Entry/Exit System (EES); an approach that this proposal seeks to reflect.
- b) ETIAS which proposed a thorough security assessment, including a check in SIS, of third-country nationals who intend to travel in the EU and are exempted from the visa obligation.

⁸⁷

Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external Borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and amending Regulation (EU) No 1077/2011 (COM(2016) 194 final).

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 2018 to 2020,
- followed by full-scale operation.

1.7. Management mode(s) planned⁸⁸

☒ **Direct management** by the Commission

- ☒ by its departments, including by its staff in the Union delegations;
- ☐ by the executive agencies

☒ **Shared management** with the Member States

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

- ☐ third countries or the bodies they have designated;
- ☐ international organisations and their agencies (to be specified);
- ☐ the EIB and the European Investment Fund;
- ☒ bodies referred to in Articles 208 and 209 of the Financial Regulation;
- ☐ public law bodies;
- ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;
- ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;
- ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.
- *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

The Commission will be responsible for the overall management of the policy and eu-LISA will be responsible for the development, operation and maintenance of the system.

SIS constitutes one single information system. Consequently, the expenses provided in two of the proposals (the current one and the Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters) should not be considered as two separate amounts but as a single one. The budgetary implications of the changes required for the implementation of both proposals are included in a single legislative financial statement.

⁸⁸

Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission, Member States and the Agency 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 Committee to implement technical and operational measures as described in this proposal.

In addition, this proposed Regulation makes provisions in Article 54(7) and (8) for a formal, regular review and evaluation process.

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.

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

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

2.2. Furthermore, eu-LISA is also now required to provide daily, monthly and annual statistics on the use of SIS, ensuring continuous monitoring of the system and its functioning against objectives. Management and control system

2.2.1. Risk(s) identified

The following risks are identified:

1. Potential difficulties for eu-LISA in managing the developments presented in the current proposal in parallel with other ongoing developments (e.g. the implementation of AFIS in SIS) and future developments (e.g. the Entry-Exit system, ETIAS and the upgrade of Eurodac). This risk could be mitigated by ensuring eu-LISA has sufficient staff and resources to carry out these tasks and the ongoing management of the Maintenance in Working Order (MWO) contractor.

2. Difficulties for the Member States:

2.1 These difficulties are primarily of a financial nature. For example, the legislative proposals include the mandatory development of a partial national copy in each N.SIS II. Member States which have not developed one already will have to make the investment. Similarly, national implementation of the Interface Control Document should be a complete implementation. Those Member States that have not yet done this will have to make provision for this in the budgets of the relevant Ministries. This risk could be mitigated through the provision of EU funding for Member States, e.g. from the Borders component of the Internal Security Fund (ISF).

2.2 The national systems have to be aligned with central requirements and discussions with Member States on this may introduce delays in the development. This risk could be mitigated through early engagement with Member States on this issue to ensure action can be taken at the appropriate time.

2.2.2. *Information concerning the internal control system set up*

The responsibilities for the central components of SIS are exercised by eu-LISA. In order to enable better monitoring of the use of SIS to analyse trends concerning migratory pressure, border management and criminal offences, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States and the Commission.

eu-LISA's accounts will be submitted for the approval of the Court of Auditors and subject to the discharge procedure. The Commission's Internal Audit Service will carry out audits in cooperation with the Agency's internal auditor.

2.2.3. *Estimate of the costs and benefits of the controls and assessment of the expected level of risk of error*

N/A

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

The measures foreseen to combat fraud are laid down in Article 35 of Regulation (EU) 1077/2011 which provides as follows:

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EC) No 1073/1999 shall apply.

2. The Agency shall accede to the Interinstitutional Agreement concerning internal investigations by the European Anti-Fraud Office (OLAF) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

3. The decisions concerning funding and the implementing agreements and instruments resulting from them shall explicitly stipulate that the Court of Auditors and OLAF may carry out, if necessary, on-the-spot checks among the recipients of the Agency's funding and the agents responsible for allocating it.

In accordance with this provision, the decision of the Management Board of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Union's interests was adopted on 28 June 2012.

DG HOME's fraud prevention and detection strategy will apply.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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			
	[Heading 3 –Security and Citizenship	Diff./Non-diff. ⁸⁹	from EFTA countries ⁹⁰	from candidate countries ⁹¹	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	18.0208 – Schengen Information System	Diff	NO	NO	YES	NO
	18.020101 – Support of border management and a common visa policy to facilitate legitimate travel	Diff	NO	NO	YES	NO
	18.0207 – 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

⁸⁹ Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

⁹⁰ EFTA: European Free Trade Association.

⁹¹ Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

Heading of multiannual financial framework	3	Security and Citizenship
--	---	--------------------------

DG HOME			Year 2018	Year 2019	Year 2020	TOTAL
• Operational appropriations						
18.0208 Schengen Information System	Commitments	(1)	6,234	1,854	1,854	9,942
	Payments	(2)	6,234	1,854	1,854	9,942
18.020101 (Borders and Visa)	Commitments	(1)		18,405	18,405	36,810
	Payments	(2)		18,405	18,405	36,810
TOTAL appropriations for DG HOME	Commitments	=1+1a +3	6,234	20,259	20,259	46,752
	Payments	=2+2a +3	6,234	20,259	20,259	46,752

EUR million (to three decimal places)

Heading of multiannual financial framework	3	Security and Citizenship
---	----------	---------------------------------

eu-LISA			Year 2018	Year 2019	Year 2020	TOTAL
• Operational appropriations						
Title 1: Staff Expenditure	Commitments	(1)	0,210	0,210	0,210	0,630
	Payments	(2)	0,210	0,210	0,210	0,630
Title 2: Infrastructure and operating expenditure	Commitments	(1a)	0	0	0	0
	Payments	(2a)	0	0	0	0
Title 3: Operational expenditure	Commitments	(1a)	12,893	2,051	1,982	16,926
	Payments	(2a)	2,500	7,893	4,651	15,044
TOTAL appropriations for eu-LISA	Commitments	=1+1a +3	13,103	2,261	2,192	17,556
	Payments	=2+2a +3	2,710	8,103	4,861	15,674

3.2.2. Estimated impact on operational appropriations

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations	Commitments	=4+ 6								

under HEADING <...> of the multiannual financial framework	Payments	=5+ 6							
--	----------	-------	--	--	--	--	--	--	--

If more than one heading is affected by the proposal / initiative:

• TOTAL operational appropriations	Commitments	(4)							
	Payments	(5)							
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)							
TOTAL appropriations under HEADINGS 1 to 4 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	19,337	22,520	22,451				64,308
	Payments	=5+ 6	8,944	28,362	25,120				62,426

3.2.3. *Estimated impact on appropriations of an administrative nature*

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 N ⁹²	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
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments							
	Payments							

⁹²

Year N is the year in which implementation of the proposal/initiative starts.

3.2.3.1. Estimated impact on eu-LISA's operational appropriations

- ☐ The proposal/initiative does not require the use of operational appropriations
- ☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Indicate objectives and outputs ↓			Year 2018		Year 2019		Year 2020		Enter as many years as necessary to show the duration of the impact (see point 1.6)						TOTAL			
	OUTPUTS																	
	Type ⁹³	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 ⁹⁴ Development Central System																		
- Contractor			1	5,013														5,013
- Software			1	4,050														4,050
- Hardware			1	3,692														3,692
Subtotal for specific objective No 1				12,755														12,755
SPECIFIC OBJECTIVE No 2 Maintenance Central System																		
-Contractor			1	0	1	0,365	1	0,365										0,730
Software			1	0	1	0,810	1	0,810										1,620
Hardware			1	0	1	0,738	1	0,738										1,476
Subtotal for specific objective No 2						1,913		1,913										3,826

⁹³

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

⁹⁴

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

SPECIFIC OBJECTIVE No 3 Meetings/Training																
Training activities	1	0,138	1	0,138	1	0,069										0,345
Subtotal for specific objective No 3		0,138		0,138		0,069										0,345
TOTAL COST		12,893		2,051		1,982										16,926

Commitment appropriations in EUR million (to three decimal places)

3.2.3.2. Estimated impact on DG HOME appropriations

- ☐ The proposal/initiative does not require the use of operational appropriations
- ☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Indicate objectives and outputs ↓			Year 2018		Year 2019		Year 2020		Enter as many years as necessary to show the duration of the impact (see point 1.6)						TOTAL			
	OUTPUTS																	
	Type ⁹⁵	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 ⁹⁶ Development National System			1		1	1,221	1	1,221										2,442
SPECIFIC OBJECTIVE No 2 Infrastructure			1		1	17,184	1	17,184										34,368
TOTAL COST						18,405		18,405										36,810

⁹⁵ Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

⁹⁶ As described in point 1.4.2. 'Specific objective(s)...'.

3.2.3.3. Estimated impact on eu-LISA's human resources - 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 2018	Year 2019	Year 2020	TOTAL
Officials (AD Grades)				
Officials (AST Grades)				
Contract staff	0,210	0,210	0,210	0,630
Temporary staff				
Seconded National Experts				
TOTAL	0,210	0,210	0,210	0,630

Recruitment is planned for January 2018. All staff must be available as of early 2018 in order to allow starting the development in due time with a view of ensuring an entry into operations of SIS II Recast in 2020. The 3 new Contractual Agents (CAs) are needed to cover needs both for the project implementation as well as for operational support and maintenance after deployment to production. These resources will be used to:

- Support the project implementation as project team members, including activities as: the definition of requirements and technical specifications, cooperation and support to Member States during the implementation; updates of the Interface Control Document (ICD), the follow-up of the contractual deliveries, documentation delivery and updates, etc.
- Support transition activities for putting the system into operations in cooperation with the contractor (releases follow-up, operational process updates, trainings (including Member States training activities), etc.
- Support the longer-term activities, definition of specifications, contractual preparations in case there is reengineering of the system (e.g. due to image recognition) or in case the new SIS II Maintenance in Working Order (MWO) contract will need to be amended to cover additional changes (from technical and budgetary perspective)
- Enforce the second level support following Entry into Operation (EiO), during continuous maintenance and operations

It has to be noted that the three new resources (FTE CA) will act on top of the internal teams resources which will be as well dedicated to the project/contractual and financial follow-up/operational activities. The use of CAs will provide adequate duration and continuity of the

contracts to ensure business continuity and use of the same specialised people for operational support activities after the project conclusion. On top of that, the operational support activities require accesses to Production environment that cannot be assigned to contractors or external staff.

3.2.3.4. Estimated requirements of human resources

- ☐ The proposal/initiative does not require the use of human resources.
- ☐ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

	Year N	Year N+1	Year N+2	Year N+3	Enter as many years as necessa ry to show the duratio n 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)⁹⁷							
XX 01 02 01 (AC, END, INT from the 'global envelope')							
XX 01 02 02 (AC, AL, END, INT and JED in the delegations)							
XX 01 04 yy ⁹⁸	- at Headquarters						
	- 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 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	

⁹⁷ AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JED= Junior Experts in Delegations.

⁹⁸ Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.4. *Compatibility with the current multiannual financial framework*

- ☐ The proposal/initiative is compatible the current multiannual financial framework.
- ☒ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

A re-programming of the remainder of the Smart Borders envelope of the Internal Security Fund is planned in order to implement the functionalities and changes foreseen in the two proposals. The ISF Borders Regulation is the financial instrument where the budget for the implementation of the Smart Borders package has been included. In Article 5 it provides that EUR 791 million shall be implemented through a programme for setting up IT systems supporting the management of migration flows across the external border under the conditions laid down in Article 15. Out of the above-mentioned EUR 791 million, EUR 480 million is reserved for the development of the Entry-Exit System and EUR 210 million for the development of the European Travel Information and Authorisation System (ETIAS). The remainder, EUR 100.828 million will be partly used to cover the costs for the changes, foreseen in the two proposals.

- ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework.

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:

Appropriations in 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								

3.3. Estimated impact on revenue

- ☐ The proposal/initiative has no financial impact on revenue.
- ☒ The proposal/initiative has the following financial impact:
 - ☐ on own resources
 - ☒ on miscellaneous revenue

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative ⁹⁹						
		2018	2019	2020	2021	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article 6313 – contribution Schengen Associated Countries (CH, NO, LI, IS).		p.m	p.m	p.m	p.m			

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

18.02.08 (Schengen Information System), 18.02.07 (eu-LISA)

Specify the method for calculating the impact on revenue.

The budget shall include a contribution from countries associated with the implementation, application and development of the Schengen acquis.

⁹⁹

As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25 % for collection costs.