Basic information

2016/0408(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Schengen Information System (SIS) in the field of border checks Repealing Regulation (EC) No 1987/2006 2005/0106(COD) See also 2016/0407(COD) See also 2016/0409(COD) Amended by 2019/0002(COD) **Subject** 7.10.04 External borders crossing and controls, visas	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	COELHO Carlos (PPE)	09/03/2017
	Shadow rapporteur DALLI Miriam (S&D) HALLA-AHO Jussi (ECR) DEPREZ Gérard (ALDE) VERGIAT Marie-Christine (GUE/NGL) JOLY Eva (Verts/ALE) MEUTHEN Jörg (EFDD) FONTANA Lorenzo (ENF)	

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	VAUTMANS Hilde (ALDE)	15/05/2017
BUDG Budgets	The committee decided not to give an opinion.	

Council of the European Union

Council configuration	Meetings	Date
Transport, Telecommunications and Energy	3545	2017-06-09
Agriculture and Fisheries	3651	2018-11-19

European Commission	Commission DG	Commissioner
	Migration and Home Affairs	AVRAMOPOULOS Dimitris

Key events

Date	Event	Reference	Summary
21/12/2016	Legislative proposal published	COM(2016)0882	Summary
06/04/2017	Committee referral announced in Parliament, 1st reading		
09/06/2017	Debate in Council		
06/11/2017	Vote in committee, 1st reading		
06/11/2017	Committee decision to open interinstitutional negotiations with report adopted in committee		
10/11/2017	Committee report tabled for plenary, 1st reading	A8-0347/2017	Summary
13/11/2017	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
15/11/2017	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
23/10/2018	Debate in Parliament		
24/10/2018	Decision by Parliament, 1st reading	T8-0412/2018	Summary
24/10/2018	Results of vote in Parliament		
19/11/2018	Act adopted by Council after Parliament's 1st reading		
28/11/2018	Final act signed		
28/11/2018	End of procedure in Parliament		
07/12/2018	Final act published in Official Journal		

Technical information

Procedure reference	2016/0408(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Repealing Regulation (EC) No 1987/2006 2005/0106(COD) See also 2016/0407(COD) See also 2016/0409(COD) Amended by 2019/0002(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 079-p2 Treaty on the Functioning of the EU TFEU 077-p2
Other legal basis	Rules of Procedure EP 165
Stage reached in procedure	Procedure completed

Committee dossier	LIBE/8/08856

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE606.234	27/06/2017	
Committee opinion	AFET	PE605.920	26/07/2017	
Amendments tabled in committee		PE609.653	18/09/2017	
Committee report tabled for plenary, 1st reading/single reading		A8-0347/2017	10/11/2017	Summary
Text adopted by Parliament, 1st reading/single reading		T8-0412/2018	24/10/2018	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00035/2018/LEX	28/11/2018	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2016)0882	21/12/2016	Summary
Commission response to text adopted in plenary	SP(2018)755	21/11/2018	
Follow-up document	COM(2020)0072	28/02/2020	
Follow-up document	COM(2021)0336	29/06/2021	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	ES_PARLIAMENT	COM(2016)0882	23/05/2017	
Contribution	PT_PARLIAMENT	COM(2016)0882	29/05/2017	
Contribution	IT_SENATE	COM(2016)0882	06/06/2017	
Contribution	CZ_SENATE	COM(2016)0882	13/06/2017	
Contribution	IT_CHAMBER	COM(2016)0882	04/08/2017	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary

EDPS	Document attached to the procedure	N8-0046/2017 OJ C 200 23.06.2017, p. 0014	03/05/2017	

Additional information		
Source	**Document**	**Date**
EP Research Service	Briefing	

Final act

Corrigendum to final act 32018R1861R(03)
OJ L 288 03.09.2020, p. 0029

Regulation 2018/1861
OJ L 312 07.12.2018, p. 0014 Summary

Schengen Information System (SIS) in the field of border checks

2016/0408(COD) - 28/11/2018 - Final act

PURPOSE: to improve the Schengen Information System (SIS) in the field of border checks with a view to making it more efficient, strengthening data protection and extending rights of access.

LEGISLATIVE ACT: Regulation (EU) 2018/1861 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 amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

CONTENT: 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. This Regulation:

- establishes the conditions and procedures for the entry and processing of alerts in SIS on third-country nationals and for the exchange of supplementary information and additional data for the purpose of refusing entry into and stay on the territory of the Member States;

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

The Regulation is accompanied by two other Regulations on the use of the SIS: (i) in the field of police and judicial cooperation in criminal matters; (ii) for the purpose of returning illegally staying third-country nationals.

Architecture

SIS comprises a central system (Central SIS) and national systems. National systems may contain a full or partial copy of the SIS database, which may be shared by two or more Member States. The Central SIS and the communication infrastructure will have to be managed so as to ensure their functioning 24 hours a day, 7 days a week. For this reason, the Agency "eu-LISA" will implement technical solutions to reinforce the continuous availability of SIS.

New categories of data

New data categories are introduced in SIS to allow end-users to take informed decisions based upon an alert without losing time. Alerts for refusal of entry and stay should contain information concerning the decision on which the alert is based. Furthermore, in order to facilitate identification and detect multiple identities, the alert should, where such information is available, include a reference to the personal identification document of the individual concerned or its number and a copy, if possible in colour, of the document.

Alerts for refusal of entry and stay

An alert may be entered only if the Member State has taken an administrative or judicial decision and has concluded, after an individual assessment, that the third-country national poses a threat to public policy or public security or to national security, namely when:

- a third-country national has been convicted in a Member State of an offence punishable by deprivation of liberty for at least one year;

- there are serious reasons to believe that a third-country national has committed a serious criminal offence, including a terrorist offence or if it appears that he intends to commit such an offence in the territory of a Member State;

- a third-country national has circumvented or attempted to circumvent national or Union law on entry and residence in the territory of the Member States.

The issuing Member State shall ensure that the alert takes effect in SIS as soon as the third-country national concerned has left the territory of the Member States.

Biometric data

SIS will permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. Any entry of photographs, facial images or dactyloscopic data into SIS and any use of such data should: (i) be limited to what is necessary for the objectives pursued, (ii) be authorised by Union law, (iii) respect fundamental rights, including the best interests of the child, and (iv) be in accordance with Union law on data protection.

In order to avoid inconveniences caused by misidentification, SIS should also allow for the processing of data concerning individuals whose identity has been misused, subject to suitable safeguards, to obtaining the consent of the individual concerned for each data category, in particular palm prints, and to a strict limitation of the purposes for which such personal data can be lawfully processed.

Period for keeping alerts

An issuing Member State shall, within three years of the entry of an alert into SIS, review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five years.

Access to data

Europol will have access to all categories of data contained in the SIS and may exchange additional information with the SIRENE Bureaux of the Member States. In addition, Member States must inform Europol of any positive response when a person is wanted in connection with a terrorist offense. The European Border and Coast Guard Agency will also have access to the different categories of alerts in the SIS. This will allow Europol's European Counter Terrorism Centre to check if there is any additional relevant information available in Europol's databases.

For the purposes set out in its mandate, the European Border and Coast Guard Agency will also have access to the alert categories in SIS.

ENTRY INTO FORCE : 27.12.2018.

By 28.12.2021, the Commission shall adopt a decision setting the date on which the SIS is put into service under the Regulation after verifying that the relevant conditions are fulfilled.

Schengen Information System (SIS) in the field of border checks

2016/0408(COD) - 21/12/2016 - Legislative proposal

PURPOSE: to reform the Schengen Information System (SIS) in order to enhance the general provisions of EU border management.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: in 2016, the Commission carried out a comprehensive evaluation of SIS, three years after the entry into operation of its second generation. This evaluation showed that SIS has been a genuine operational success.

Nonetheless, 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.

These proposals cover the use of the system for:

- **border management**,
- police cooperation and judicial cooperation in criminal matters, and
- the return of illegally staying third country nationals.

CONTENT: the present proposal and the supplementary proposal on the use of the SIS for police and judicial cooperation in criminal matters lay down rules covering the comprehensive end-to-end use of SIS, including the Central SIS managed by eu-LISA Agency, but also the needs of the end-user.

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. This proposal as well as the parallel 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.

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.

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. 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.

The proposal empowers eu-LISA to produce data quality reports to Member States at regular intervals.

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 existing Regulation. Two new 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 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. Palm prints can be used to establish a person's identity in the same way that fingerprints can be used.

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 section is intended to describe the new elements in access rights with regard to EU Agencies (institutional users). Appropriate safeguards are put in place to ensure that the data in the system is properly protected (including the provisions requiring that these bodies may only access the data they need to carry out their tasks).

The access rights of competent national authorities have not been amended.

Refusal of entry and stay: currently, 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. With the new proposal, it shall be required 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** (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).

This proposal is closely linked with the Commission proposal concerning the use of SIS for the return of illegally staying third country nationals.

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 which was not obligatory in the former legislation.

Data protection and security: the 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. It provides that the Commission remains responsible for the contractual management of the SIS communication infrastructure, including tasks which will be transferred to eu-LISA.

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 that can be held about people for whom an alert has been issued.

The proposal also 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.

The proposal sets out the rights for data subjects to access data, rectify inaccurate data and erase unlawfully stored data.

Lastly, provisions are laid down as regards statistics on the use of the SIS.

BUDGETARY IMPLICATIONS: the estimated cost is **EUR 64.3 million** from 2018-2020.

Schengen Information System (SIS) in the field of border checks

2016/0408(COD) - 10/11/2017 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Carlos COELHO (EPP, PT) on the 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 committee recommended that Parliament's position adopted in first reading following the ordinary legislative procedure should amend the Commission proposal as follows:

System architecture: the Commission's proposal requires all Member States to have a national copy containing a complete or partial copy of the SIS database as well as a backup N.SIS. Given the risk to data security, Members believe that **Member States should not be required to have a national copy** in order to ensure the availability of the system. As an additional means of ensuring the uninterrupted availability of the SIS, Members proposed that a **back-up communication infrastructure** be developed and used in case of failure of the main communication infrastructure. In particular, the "CS-CIS" (containing the SIS database) or its backup version **should contain an additional copy of the SIS database and be used simultaneously in active operation.**

The CS-SIS and its back-up version should be installed at the technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (the "Eu-LISA agency").

Member States' responsibilities: each Member State shall designate a national authority which is operational **24 hours a day, 7 days a week** and shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau). **The SIRENE Bureau** shall serve as single contact point for Member States to exchange supplementary information regarding alerts.

The SIRENE Bureaux shall substantially reply to a request for supplementary information not later than **six hours** after the receipt of the request. In case of alerts for terrorist offences and in cases of alerts concerning, the SIRENE Bureaux shall act immediately.

To further increase the quality of data in SIS, the Agency should also offer **training on the use of SIS** to national training bodies and, insofar as possible, to SIRENE staff and to end-users.

Access to the system: the Commission proposal provides for increased access opportunities for a range of European agencies such as Europol, Eurojust, and the European Border and Coast Guard Agency. The amendments introduced aim to clarify, with regard to the existing mandates of the different agencies, the circumstances in which it is possible to access the SIS data. It is also proposed to strengthen the safeguards in this respect, whether in terms of prior training or logging or oversight, indicating in particular, the date and time of the data processing activity, the type of data processed and the name of the person responsible for data processing.

Data security: Members specified that 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, that: (i) deny unauthorised persons access to data-processing equipment and facilities used for processing personal data; (ii) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS; (iii) ensure that the installed system may, in case of interruption, be restored; (iv) ensure that faults are reported and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning.

In order to prevent the piracy of SIS by an external service provider, Members proposed that Member States cooperating with external contractors on any SIS-related tasks **closely monitor contractors' activities** to ensure compliance with all provisions of the Regulation, including in particular security, confidentiality and data protection.

Data protection: access to the system should be subject to all the legal provisions applicable to national data protection authorities and to the possibility for the supervisory authorities to verify the correct application of the legal provisions, in particular through the evaluation mechanism of Schengen introduced by Council Regulation (EU) No 1053/2013.

Members proposed a series of amendments that mainly aim to clarify what the applicable rules are. In addition, a number of provisions are strengthened and **brought further in line with EU data protection framework.**

According to the amended text, any introduction and use in the SIS of **photographs, facial images and dactyloscopic data** should (i) remain within the limits of what is strictly necessary to achieve the objectives pursued; (ii) be authorised by Union law; (iii) respect fundamental rights, including the best interests of the child, and (iv) be in accordance with relevant provisions on data protection laid down in the SIS legal instruments, Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council.

Data entered in the SIS **should not reveal sensitive information** about the person, such as ethnicity, religion, disability, gender or sexual orientation.

Alerts on refusal of entry and stay: an alert for the purpose of refusing entry and stay shall be issued **after a national decision** and only:

- if a third-country national has been convicted in a Member State of an offence carrying a penalty involving the **deprivation of liberty of at least three years**;
- if there are serious grounds for believing that a third-country national has **committed a serious crime or terrorist offence** or there is evidence that a third-country national intends to commit such an offence in the territory of a Member State.

The Member State shall then take an administrative or judicial decision if it concludes, after an individual assessment, that the third-country national poses a threat to public policy or public security or national security.

Only then could the Member State issue the alert for non-admission.

Consultation using biometric data: Members pointed out that **fingerprint data** stored in the SIS should only be used for identification purposes if the identity of the person cannot be established by alphanumeric data (name, first name, date of birth). To this end, the central SIS should contain an automated fingerprint identification system.

Retention period of alerts: The time limit for reviewing personal alerts should be **three years maximum.** As a general principle, alerts should be automatically deleted from the SIS after three years.

Entry into force of the new provisions: in order to avoid long delays, as was the case with the SIS II legal framework, Members proposed that the new legal framework be implemented **one year** after its entry into force.

Schengen Information System (SIS) in the field of border checks

2016/0408(COD) - 24/10/2018 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 530 votes to 50, with 66 abstentions, a legislative resolution on the 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's position adopted at first reading under the ordinary legislative procedure amended the Commission proposal as follows:

Purpose: the proposed Regulation seeks to introduce a **series of improvements** to SIS which shall increase its effectiveness, strengthen data protection and extend access rights. It establishes the conditions and procedures for the entry and processing of alerts in SIS on third-country nationals and for the exchange of supplementary information and additional data for the purpose of refusing entry into and stay on the territory of the Member States.

Technical architecture: SIS includes a central system (Central SIS) and national systems. The national systems may contain a complete or partial copy of the SIS database, which may be shared by two or more Member States. **The availability of SIS** shall be subject to close monitoring at central and Member State level and any incident of unavailability for end-users shall be registered and reported to stakeholders at national and Union level. Each Member State shall set up a **backup** for its national system.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) shall implement technical solutions to reinforce the uninterrupted availability of SIS.

Costs: the amended text provides that funding shall be allocated from the envelope of **EUR 791 million** foreseen under Regulation (EU) No 515/2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa, to cover the costs of implementation of this Regulation. From this envelope, an amount of EUR 31 098 000 is allocated to eu-LISA. Member States shall receive an additional global allocation of EUR 36 810 000 to be distributed in equal shares through a lump sum to their basic allocation.

Member States' responsibilities: each Member State shall designate a national authority which is **operational 24 hours a day, 7 days a week** and shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau). The SIRENE Bureau shall serve as **single contact point** for Member States to exchange supplementary information regarding alerts.

Each SIRENE Bureau shall, in accordance with national law, have easy **direct or indirect access** to all relevant national information, including national databases and all information on its Member States' alerts, and to expert advice, in order to be able to react to requests for supplementary information swiftly and within the deadlines. Member States shall ensure that end-users and the staff of the SIRENE Bureaux regularly receive **training**, including on data security, data protection and data quality.

Data security: Parliament specified that **national plans for security**, business continuity and disaster recovery shall ensure that: (i) **unauthorised processing** of data in the SIS and any unauthorised modification or erasure of data processed in the SIS is prevented; (ii) systems installed in the event of an interruption are **restored**; (iii) the SIS correctly performs its functions, that faults are reported and **personal data** stored in SIS cannot be corrupted by means of the system malfunctioning.

Where a Member State cooperates with **external contractors** in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular on security, confidentiality and data protection.

Categories of data: the amended text provides for the introduction of new categories of data in the SIS to enable end-users to make informed decisions based on an alert without losing time.

In order to facilitate identification and detect multiple identities, the alert shall, where such information is available, include a reference to the **personal identification document** of the individual concerned or its number and a copy, if possible in colour, of the document. Where available, all the relevant data, in particular the **forename** of the individual concerned, shall be inserted when creating an alert.

Alerts on refusal of entry and stay: an alert may only be entered if the Member State has taken an administrative or judicial decision and has concluded, after an individual assessment, that the third-country national constitutes a threat to public policy or public security or national security, namely where:

- a third-country national has been convicted in a Member State of an offence carrying a penalty involving the **deprivation of liberty of at least one year**;
- there are serious grounds for believing that a third-country national has committed a **serious criminal offence, including a terrorist offence**, or there are clear indications of his or her intention to commit such an offence in the territory of a Member State;
- a third-country national has **circumvented or attempted to circumvent Union or national law** on entry into and stay on the territory of the Member States.

Retention period: within **three years** of entry of an alert into SIS, the issuing Member State shall review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five years.

Biometric data: under the proposed Regulation, SIS shall permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned.

Parliament has specified that any entry of photographs, facial images or dactyloscopic data into SIS and any use of such data shall: (i) be **limited to what is necessary** for the objectives pursued; (ii) be authorised by Union law; (iii) respect **fundamental rights**, including the best interests of the child; (iv) be in accordance with Union law on **data protection**.

Access to the system: the proposed Regulation provides for enhanced access possibilities for a range of European agencies such as Europol, Eurojust, and the European Border and Coast Guard Agency.

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 are encouraged to **share information on terrorism-related activity with Europol**. This information sharing should be carried out through the exchange of supplementary information with Europol on the alerts concerned.