Basic information

2016/0409(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters Repealing Decision 2007/533/JHA 2005/0103(CNS) Repealing Regulation (EC) No 1986/2006 2005/0104(COD) Amended by 2018/0152B(COD) Amended by 2019/0001A(COD) Amended by 2019/0001B(COD) See also 2016/0408(COD) **Subject** 7.10.04 External borders crossing and controls, visas 7.30.05 Police cooperation 7.40.04 Judicial cooperation in criminal matters	

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	The committee decided not to give an opinion.	
BUDG Budgets	The committee decided not to give an opinion.	
TRAN Transport and Tourism	The committee decided not to give an opinion.	

	JURI Legal Affairs	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)0883	Summary
06/04/2017	Committee referral announced in Parliament, 1st reading		
09/06/2017	Debate in Council		
19/10/2017	Committee decision to open interinstitutional negotiations with report adopted in committee		
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	A8-0349/2017	Summary
13/11/2017	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 72)		
15/11/2017	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 72)		
23/10/2018	Debate in Parliament		
24/10/2018	Decision by Parliament, 1st reading	T8-0413/2018	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	2016/0409(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Repealing Decision 2007/533/JHA 2005/0103(CNS) Repealing Regulation (EC) No 1986/2006 2005/0104(COD) Amended by 2018/0152B(COD) Amended by 2019/0001A(COD) Amended by 2019/0001B(COD) See also 2016/0408(COD)
Legal basis	Treaty on the Functioning of the European Union TFEU 087-p2 Treaty on the Functioning of the European Union TFEU 085-p1-a3 Treaty on the Functioning of the European Union TFEU 082-p1 Treaty on the Functioning of the European Union TFEU 088-p2-a2
Other legal basis	Rules of Procedure EP 165
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/8/08847

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE606.235	27/06/2017	
Amendments tabled in committee		PE609.654	07/09/2017	
Amendments tabled in committee		PE610.562	07/09/2017	
Committee report tabled for plenary, 1st reading/single reading		A8-0349/2017	10/11/2017	Summary
Text adopted by Parliament, 1st reading/single reading		T8-0413/2018	24/10/2018	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00036/2018/LEX	28/11/2018	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2016)0883	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)0883	23/05/2017	
Contribution	PT_PARLIAMENT	COM(2016)0883	29/05/2017	
Contribution	IT_SENATE	COM(2016)0883	06/06/2017	
Contribution	CZ_SENATE	COM(2016)0883	13/06/2017	
Contribution	IT_CHAMBER	COM(2016)0883	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
European Parliament	Briefing	
European Commission	EUR-Lex	

Final act

Regulation 2018/1862
OJ L 312 07.12.2018, p. 0056 Summary

Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters

2016/0409(COD) - 24/10/2018 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 555 votes to 67, with 20 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 police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU.

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 **persons and objects** and for the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.

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.

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: alerts on the following categories of persons shall be entered in SIS at the request of the competent authority of the issuing Member State:

- missing persons who need to be placed under protection for their own protection and in order to prevent a threat to public order or public security;
- children at risk of abduction by a parent, a family member or a guardian, who need to be prevented from travelling;
- children who need to be prevented from travelling owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and (i) becoming victims of trafficking in human beings, or of forced marriage, female genital mutilation or other forms of gender-based violence; (ii) becoming victims of or involved in terrorist offences; or (iii) becoming conscripted or enlisted into armed groups;
- vulnerable persons who are of age and who need to be prevented from travelling for their own protection owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings or gender-based violence.

Actions and decisions by the competent authorities, including judicial authorities, following an alert on a child should be taken in cooperation with child protection authorities. The national **hotline** for missing children should be informed, where appropriate.

Within **three years** of entering an alert in the SIS, the issuing Member State shall review the need to keep it.

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**.

It would also be possible to add a **DNA profile** to an alert in clearly defined cases where fingerprint data are not available. This DNA profile shall only be accessible to authorised users.

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.

The amendments adopted aim to clarify, with regard to the existing mandates of the different agencies, the circumstances under which access to SIS data is possible.

Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters

2016/0409(COD) - 21/12/2016 - Legislative proposal

PURPOSE: to reform the Schengen Information System (SIS) in order to enhance the general provisions regarding police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU.

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 border management 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 proposal on border management 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.

In cases where fingerprints or palm prints are not available, the proposal allows for the use of DNA profiles for missing persons who need to be placed under protection, especially children. This functionality will be used only in the absence of fingerprints and will be accessible only to authorised users.

The proposed changes will also allow **SIS alerts to be issued for unknown persons** wanted in connection with a crime, based on fingerprints or palm prints. This new alert category complements the Prüm provisions that enable interconnectivity of national criminal fingerprint identification systems. Via the Prüm mechanism, a Member State can launch a request to ascertain if the perpetrator of a crime whose fingerprints have been found is known in any other Member State (usually for investigative purposes). A person can be identified via the Prüm mechanism only if he or she has been fingerprinted in another Member State for criminal purposes. Hence, first time offenders cannot be identified.

Under this proposal, the **storage of fingerprints of unknown wanted persons**, will enable the fingerprints of an unknown perpetrator to be uploaded into SIS so that he or she can be identified as wanted if encountered in another Member State.

It should be noted that the use of this functionality presupposes that the Member States conducted a prior consultation of all available national and international sources but could not ascertain the identity of the person concerned.

Access to SIS by immigration authorities – institutional users: users such as Europol, Eurojust and the European Border and Coast Guard Agency shall have 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 requiring that these bodies may only access the data they need to carry out their tasks.

Provisions are also laid down enabling immigration authorities to access SIS.

Suspension of certain alerts: the proposal provides for Member States to temporarily suspend alerts for arrest (in case of an ongoing police operation or investigation), making them visible only to SIRENE Bureaux but not to the officers on the ground for a limited period of time. This provision helps to avoid that a confidential police operation to arrest a highly wanted offender is jeopardised by a police officer who is not involved in the matter.

Provisions are laid down for alerts on missing persons. Changes to these allow **preventive alerts** to be issued in cases where **parental abduction** is deemed a high risk, and provide for more finely tuned categorisation of missing persons alerts. These changes will mean that, where there is a high risk of imminent parental abduction, border guards and law enforcement officials are made aware of the risk and will be able to examine more closely

the circumstances where an at-risk child is travelling, taking the child into protective custody if required. This alert will require an appropriate decision of the judicial authorities granting custody only to one of the parents.

Inquiry check: the proposal introduces a new form of check, the 'inquiry check'. This is, in particular, intended to support measures to counter terrorism and serious crime. It allows authorities to stop and question the person concerned. It is more in-depth than the existing discreet check, but does not involve searching the person and does not amount to arresting him or her. It may, however, provide sufficient information to decide on further action to be taken.

An expanded list of objects is set out for which alerts can be issued, adding falsified documents, falsified banknotes, IT equipment, component parts of vehicles, etc.

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 police cooperation and judicial cooperation in criminal matters

2016/0409(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 police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU

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.

Europol should be immediately informed by Member States of all alerts created and positive replies to these alerts when a person or object is wanted by a Member State in relation to an offense referred to in Directive (EU) 2017/541 the fight against terrorism.

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,** particularly 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.

Specific amendments regarding alerts: Members pointed out that an alert should be introduced when a suspect is wanted in connection with an alleged terrorist offense. They also delineated the use of **DNA data** and defined the circumstances in which they can accompany an alert.

Missing persons: the category of children at risk of being abducted, including by a family member, or of being removed from the Member State for the purpose of torture, sexual or gender-based violence or of being victims of activities listed in Directive (EU) 2017/541 should be introduced in the SIS.

An alert concerning a **child at risk** should be entered, following a decision of the competent judicial authority of the Member State that has jurisdiction in matters of parental responsibility where a risk exists that the child may be unlawfully and imminently removed from the Member State where that competent judicial authority is situated.

In the case of children subject to alerts, the executing Member State shall consult without delay the issuing Member State including its child protection authorities in order to agree without delay and at the latest **within 12 hours** on the measures to be taken in order to safeguard the best interest of the child.

The data entered in SIS must indicate which category the missing child at risk falls into, these being: (i) runaways; (ii) **unaccompanied children in the context of migration**; (iii) children abducted by a family member.

Investigative controls: due to their nature these should be mandatory, in full compliance with all procedural safeguards. Members have tightened up the information requirements that Member States are required to provide to enable the competent authorities of the executing Member State to take action.

This information should be **transmitted immediately** to the issuing authority when border checks or verification, police and customs checks or other enforcement actions are carried out within a Member State.

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 police cooperation and judicial cooperation in criminal matters

2016/0409(COD) - 28/11/2018 - Final act

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

LEGISLATIVE ACT: Regulation (EU) 2018/1862 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 matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010 /261/EU.

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 persons and objects and for the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters;

- 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 SIS: (i) in the field of border checks; (ii) for the return of 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 category of alerts

The following are introduced into the system:

- alerts issued for the purpose of inquiry checks, an intermediary step between discreet checks and specific checks, which allow for individuals to be interviewed.

- alerts on unknown suspects or wanted persons, which provide for the introduction into the SIS of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist incidents and which are considered to belong to a perpetrator.

- alerts of children at risk of parental abduction, and alerts on children and vulnerable adults who need to be prevented from travelling for their own protection (e.g. when travel may lead to a risk of forced marriage, female genital mutilation, trafficking in human beings).

In the case of children, these alerts and the corresponding procedures should serve the best interests of the child. Such decisions shall be made immediately and not later than 12 hours after the child was located, in consultation with relevant child protection authorities, as appropriate.

The Regulation also permits the introduction of alerts concerning objects for seizure or as evidence in criminal proceedings, such as forged documents and high value objects, as well as computer equipment.

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. Therefore, 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. If available, all relevant data, in particular the first name of the person concerned, must be inserted when creating an alert.

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.

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.

ENTRY INTO FORCE: 27.12.2018.

By 28.12.2021, the Commission will 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.