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

REGULATION (EU) 2018/1862 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 28 November 2018

on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular point (d) of the second subparagraph of Article 82(1), Article 85(1), Article 87(2)(a) and Article 88(2)(a) 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[(1)],

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 Union by supporting operational cooperation between national competent authorities, in particular border guards, the police, customs authorities, immigration authorities, and authorities responsible for the prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties.

(2) SIS was initially 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 borders[(2)] (the Convention implementing the Schengen Agreement). The development of the second generation of SIS (SIS II) was entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[(3)] and Council Decision 2001/886/JHA[(4)]. It was later established by Regulation (EC) No 1987/2006 of the European Parliament

Changes to legislation: *There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

and of the Council[5] and by Council Decision 2007/533/JHA[6]. SIS II replaced SIS as created pursuant to the Convention implementing the Schengen Agreement.

(3) Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system in accordance with Regulation (EC) No 1987/2006 and Decision 2007/533/JHA. On 21 December 2016, the Commission submitted the Report on the Evaluation of the Second Generation Schengen Information System (SIS II) in accordance with Articles 24(5), 43(3) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59(3) and 66(5) of Decision 2007/533/JHA and an accompanying staff working document to the European Parliament and to the Council. The recommendations set out in those documents should be reflected, as appropriate, in this Regulation.

(4) This Regulation constitutes the legal basis for SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of Part Three of the Treaty on Functioning of the European Union (TFEU). Regulation (EU) 2018/1861 of the European Parliament and of the Council[7] constitutes the legal basis for SIS in respect of matters falling within the scope of Chapter 2 of Title V of Part Three TFEU.

(5) The fact that the legal basis for SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such. It should include a single network of national offices called SIRENE Bureaux for ensuring the exchange of supplementary information. Certain provisions of those instruments should therefore be identical.

(6) It is necessary to specify the objectives of SIS, certain elements of its technical architecture and its financing, to lay down rules concerning its end-to-end operation and use and to define responsibilities. It is also necessary to determine the categories of data to be entered into the system, the purposes for which the data are to be entered and processed and the criteria for their entry. Rules are also required to govern the deletion of alerts, the authorities authorised to access the data, the use of biometric data and to further determine data protection and data processing rules.

(7) Alerts in SIS contain only the information necessary to identify a person or an object and for the action to be taken. Member States should therefore exchange supplementary information related to alerts where required.

(8) SIS includes a central system (Central SIS) and national systems. The national systems might contain a complete or partial copy of the SIS database, which may be shared by two or more Member States. Considering that SIS is the most important information exchange instrument in Europe for ensuring security and effective border management, it is necessary to ensure its uninterrupted operation at central as well as at national level. The availability of SIS should be subject to close monitoring at central and Member State level and any incident of unavailability for end-users should be registered and reported to stakeholders at national and Union level. Each Member State should set up a backup for its national system. Member States should also ensure uninterrupted connectivity with Central SIS by having duplicated and physically and geographically separated connection points. Central SIS and the Communication Infrastructure should be operated in such a way that their functioning 24 hours a day, 7 days a week is ensured. For that reason the European Union Agency for the Operational Management of Large-

***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA'), established by Regulation (EU) 2018/1726 of the European Parliament and of the Council[(8)] should implement technical solutions to reinforce the uninterrupted availability of SIS, subject to an independent impact assessment and cost-benefit analysis.

(9) It is necessary to maintain a manual setting out the detailed rules for the exchange of supplementary information concerning the actions called for by alerts ('the SIRENE Manual'). The SIRENE Bureaux, should ensure the exchange of such information in a fast and efficient manner.

(10) In order to ensure the efficient exchange of supplementary information, including on the action to be taken specified in alerts, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning the available resources and user training and the response time to inquiries they receive from other SIRENE Bureaux.

(11) Member States should ensure that the staff of their SIRENE Bureau have the linguistic skills and knowledge of relevant law and procedural rules necessary to perform their tasks.

(12) In order to be able to fully benefit from the functionalities of SIS, Member States should ensure that end-users and the staff of the SIRENE Bureaux regularly receive training, including on data security, data protection and data quality. SIRENE Bureaux should be involved in the development of training programmes. To the extent possible, SIRENE Bureaux should also provide for staff exchanges with other SIRENE Bureaux at least once a year. Member States are encouraged to take appropriate measures to avoid the loss of skills and experience through staff turnover.

(13) The operational management of the central components of SIS are exercised by eu-LISA. In order to enable eu-LISA to dedicate the necessary financial and personal resources covering all aspects of the operational management of Central SIS and the Communication Infrastructure, this Regulation should set out its tasks in detail, in particular with regard to the technical aspects of the exchange of supplementary information.

(14) Without prejudice to the responsibility of Member States for the accuracy of data entered into SIS and to the role of the SIRENE Bureaux as quality coordinators, eu-LISA should be responsible for reinforcing data quality by introducing a central data quality monitoring tool, and should provide reports at regular intervals to the Commission and to the Member States. The Commission should report to the European Parliament and to the Council on the data quality issues encountered. To further increase the quality of data in SIS, eu-LISA should also offer training on the use of SIS to national training bodies and, insofar as possible, to the SIRENE Bureaux and to end-users.

(15) In order to allow better monitoring of the use of SIS and to analyse trends concerning criminal offences, eu-LISA should be able to develop a state-of-the-art capability for statistical reporting to the Member States, to the European Parliament, to the Council, to the Commission, to Europol, to Eurojust and to the European Border and Coast Guard

Changes to legislation: *There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

Agency without jeopardising data integrity. Therefore, a central repository should be established. Statistics retained in or obtained from that repository should not contain any personal data. Member States should communicate statistics concerning exercise of the right of access, rectification of inaccurate data and erasure of unlawfully stored data in the framework of cooperation between supervisory authorities and the European Data Protection Supervisor under this Regulation.

(16) New data categories should be 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.

(17) Competent authorities should be able, where strictly necessary, to enter into SIS specific information relating to any specific, objective, physical characteristics of a person which are not subject to change, such as tattoos, marks or scars.

(18) Where available, all the relevant data, in particular the forename of the individual concerned, should be inserted when creating an alert, in order to minimise the risk of false hits and unnecessary operational activities.

(19) SIS should not store any data used to carry out searches with the exception of keeping logs to verify whether the search is lawful, for monitoring the lawfulness of data processing, for self-monitoring and for ensuring the proper functioning of the national systems as well as for data integrity and security.

(20) SIS should 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 be limited to what is necessary for the objectives pursued, should be authorised by Union law, should respect fundamental rights, including the best interests of the child, and should be in accordance with Union law on data protection, including the relevant provisions on data protection laid down in this Regulation. In the same perspective, 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.

(21) Member States should make the necessary technical arrangements so that each time end-users are entitled to carry out a search in a national police or immigration database, they also search SIS in parallel, subject to the principles set out in Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council[9] and Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council[10]. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better addresses the cross-border dimension of criminality and the mobility of criminals.

***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(22) This Regulation should set out the conditions for use of dactyloscopic data, photographs and facial images for identification and verification purposes. Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. Such use should be subject to a report by the Commission confirming the availability, reliability and readiness of the technology.

(23) The introduction of an automated fingerprint identification service within SIS complements the existing Prüm mechanism on mutual cross-border online access to designated national DNA databases and automated fingerprint identification systems, as set out in Council Decisions 2008/615/JHA[(11)] and 2008/616/JHA[(12)]. The SIS dactyloscopic data search allows an active search for the perpetrator. Therefore, it should be possible to upload the dactyloscopic data of an unknown perpetrator into SIS, provided that the owner of that data can be identified with a very high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if dactyloscopic data are found on the weapon or on any object used for the offence. The mere presence of the dactyloscopic data at the crime scene should not be considered as indicating a very high degree of probability that the dactyloscopic data are those of the perpetrator. A further precondition for the creation of such an alert should be that the identity of the suspect cannot be established on the basis of data from any other relevant national, Union or international database. Should a dactyloscopic data search lead to a potential match, the Member State should carry out further checks with the involvement of experts to establish whether the suspect is the owner of the prints stored in SIS, and should establish the identity of the person. The procedure should be subject to national law. Such identification could substantially contribute to the investigation and could lead to an arrest provided that all the conditions for an arrest are met.

(24) It should be allowed to search dactyloscopic data stored in SIS with complete or incomplete sets of fingerprints or palm prints found at a crime scene if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence, provided that a search is carried out simultaneously in the relevant national fingerprint databases. Particular attention should be given to the establishment of quality standards applicable to the storage of biometric data, including latent dactyloscopic data.

(25) Wherever the identity of a person cannot be ascertained by any other means, dactyloscopic data should be used to attempt identification. It should be allowed in all cases to identify a person by using dactyloscopic data.

(26) It should be possible to add a DNA profile to an alert in clearly defined cases where dactyloscopic data are not available. That DNA profile should only be accessible to authorised users. DNA profiles should facilitate the identification of missing persons in need of protection and particularly missing children, including by allowing the use of DNA profiles of direct ascendants, descendants or siblings to enable identification. DNA data should contain only the minimum information necessary for identification of the missing person.

(27) DNA profiles should only be retrieved from SIS where identification is necessary and proportionate for the purposes laid down in this Regulation. DNA profiles should not be