



Council of the European Union
General Secretariat

Brussels, 01 February 2021

**Interinstitutional files:
2020/0350(COD)**

WK 1347/2021 INIT

LIMITE

**SIRIS
ENFOPOL
COPEN
SCHENGEN
IXIM
COMIX
CODEC**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations

N° prev. doc.:	13882/20
N° Cion doc.:	COM(2020) 791 final

Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol
----------	---

Delegations will find below an informal working document consolidating the proposed amendment to the SIS Police Regulation with the text of the SIS Police Regulation as currently in force (Regulation (EU) 2018/1862).

The changes proposed by the Commission as compared to the Regulation (EU) 2018/1862 currently in force appear as ~~striketrough~~ and **bold underlined** .

The Presidency underlines that this document is of a purely working character and cannot be considered as an official consolidation of the Council's position on the proposal at any stage of its examination.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

Article 1

Amendments to Regulation (EU) 2018/1862

Article 2

Subject matter

1. 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.
2. This Regulation also lays down provisions on the technical architecture of SIS, on the responsibilities of the Member States, **the European Union Agency for Law Enforcement Cooperation ('Europol')** and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), on data processing, on the rights of the persons concerned and on liability.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

[(1)-(21)]

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

Article 24

General provisions on flagging

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

entered in accordance with Article 37a shall be added by Europol. ~~The flag shall be added by the SIRENE Bureau of the issuing Member State.’~~

2. In order to enable Member States to require that a flag be added to an alert entered in accordance with Article 26, all Member States shall be notified automatically of any new alert of that category through the exchange of supplementary information.
3. If in particularly urgent and serious cases, an issuing Member State **or Europol** requests the execution of the action, the executing Member State shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.’

‘CHAPTER IXa

ALERTS ENTERED BY EUROPOL ON PERSONS OF INTEREST

Article 37a

Objectives and conditions for entering alerts

1. Europol may enter alerts on persons in SIS for the purpose of informing end-users carrying out a search in SIS of the suspected involvement of those persons in a criminal offence in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794, as well as for the purpose of obtaining information in accordance with Article 37b of this Regulation that the person concerned has been located.
2. Europol may only enter an alert in SIS on persons who are third-country nationals on the basis of information received from a third country or an international organisation in accordance with Article 17(1)(b) of Regulation (EU) 2016/794, where the information relates to one of the following:
 - (a) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794, or who have been convicted of such an offence;
 - (b) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent in accordance with Article 3 of Regulation (EU) 2016/794.
3. Europol may only enter an alert in SIS after it has ensured all of the following:
 - (a) an analysis of the data provided in accordance with paragraph 2 confirmed the reliability of the source of information and the accuracy of the information on the person concerned, permitting Europol to determine that that person falls within the scope of paragraph 2, where necessary, after having carried out further exchanges of information with the data provider in accordance with Article 25 of Regulation (EU) 2016/794;
 - (b) a verification confirmed that entering the alert is necessary for achieving Europol’s objectives as laid down in Article 3 of Regulation (EU) 2016/794;
 - (c) a search in SIS, carried out in accordance with Article 48 of this Regulation, did not disclose the existence of an alert on the person concerned;
 - (d) a consultation, involving the sharing of information on the person concerned with Member States participating in Regulation (EU) 2016/794 in accordance with Article 7 of that Regulation, confirmed that:
 - (i) no intention was expressed by a Member State to enter an alert in SIS on the person concerned;
 - (ii) no reasoned objection was expressed by a Member State regarding the proposed entry of an alert in SIS on the person concerned by Europol.
4. Europol shall keep detailed records relating to the entry of the alert in SIS and the grounds for such entry to permit verification of compliance with the substantive and procedural requirements laid down in paragraphs 1, 2 and 3. Such records shall be available for the European Data Protection Supervisor on request.

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

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

Article 37b

Execution of the action based on an alert

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

(a) collect and communicate the following information:

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

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

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

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

Article 48

'Entry and processing of Access to data in SIS by Europol'

1. ~~The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794~~ **Europol** shall, where necessary to fulfil its mandate, have the right to access and search data in SIS **and to enter, update and delete alerts pursuant to Article 37a of this Regulation. Europol shall enter, update, delete and search SIS data through a dedicated technical interface. The technical interface shall be set up and maintained by Europol in compliance with the common standards, protocols and technical procedures defined in Article 9 of this Regulation and shall allow direct connection to Central SIS.**

Europol ~~shall~~ **may also exchange and further request** supplementary information in accordance with the provisions of the SIRENE Manual. **To that end, Europol shall ensure availability to supplementary information related to its own alerts 24 hours a day, 7 days a week.**
2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the Communication Infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States through the channels defined by Regulation (EU) 2016/794.
3. Europol may process the supplementary information that has been provided to it by Member States for the purposes of comparing it with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for the strategic, thematic or operational analyses referred to in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this Article shall be carried out in accordance with that Regulation.
4. Europol's use of information obtained from a search in SIS or from the processing of supplementary information shall be subject to the consent of the ~~issuing~~ Member State **that provided the information either as issuing Member State or as executing Member State.** If the Member State allows the use of such information, its handling by Europol shall be governed by Regulation (EU) 2016/794. Europol shall only communicate such information to third countries and third bodies with the consent of the Member State that provided the information and in full compliance with Union law on data protection.
5. Europol shall:
 - (a) without prejudice to paragraphs 4 and 6, not connect parts of SIS nor transfer the data contained in it to which it has access to any system for data collection and processing operated by or at Europol, nor download or otherwise copy any part of SIS;
 - (b) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the

- issuing and the executing Member State of the continued storage of such supplementary information and present a justification for it;
- (c) limit access to data in SIS, including supplementary information, to specifically authorised staff of Europol who require access to such data for the performance of their tasks;
- (d) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;
- (e) ensure that its staff who are authorised to process SIS data receive appropriate training and information in accordance with Article 14(1); and
- (f) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data in SIS and in the exchange and processing of supplementary information.
6. Europol shall only copy data from SIS for technical purposes where such copying is necessary in order for duly authorised Europol staff to carry out a direct search. This Regulation shall apply to such copies. The technical copy shall only 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 considered to be 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. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Europol shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12. Such logs and documentation shall not be considered to be unlawful downloading or copying of part of SIS.
- 7a. The European Data Protection Supervisor shall carry out an audit of the data processing operations of Europol under this Regulation in accordance with international auditing standards at least every four years.**

Article 53

Review period for alerts on persons

1. Alerts on persons shall be kept only for the time required to achieve the purposes for which they were entered.
2. A Member State may enter an alert on a person for the purposes of Article 26 and points (a) and (b) of Article 32(1) for a period of five years. The issuing Member State shall review the need to retain the alert within the five year period.
3. A Member State may enter an alert on a person for the purposes of Articles 34 and 40 for a period of three years. The issuing Member State shall review the need to retain the alert within the three year period.
4. A Member State may enter an alert on a person for the purposes of points (c), (d) and (e) of Article 32 (1) and of Article 36 for a period of one year. The issuing Member State shall review the need to retain the alert within the one year period.
5. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

- 5a. Europol may enter an alert on a person for the purposes of Article 37a (1) for a period of one year. Europol shall review the need to retain the alert within that period. Europol shall, where appropriate, set shorter review periods.**
6. Within the review period referred to in paragraphs 2, 3, ~~and 4~~, **5 and 5a**, the issuing Member State, **and in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol**, may, following a comprehensive individual assessment, which shall be recorded, decide to retain the alert on a person for longer than the review period, where this proves necessary and proportionate for the purposes for which the alert was entered. In such cases paragraph 2, 3, ~~or 4~~, **5 or 5a of this Article** shall also apply to the extension. Any such extension shall be communicated to CS-SIS.
7. Alerts on persons shall be deleted automatically after the review period referred to in paragraphs 2, 3, ~~and 4~~, **5 and 5a** has expired, except where the issuing Member State **or in the case of alerts entered in SIS pursuant to Article 37a of this Regulation Europol**, has informed CS-SIS of an extension pursuant to paragraph 6 of this Article. CS-SIS shall automatically inform the issuing Member State **or Europol** of the scheduled deletion of data four months in advance.
8. Member States **and Europol** shall keep statistics on the number of alerts on persons the retention periods of which have been extended in accordance with paragraph 6 of this Article and transmit them, upon request, to the supervisory authorities referred to in Article 69.

Article 55

Deletion of alerts

1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted when the person has been surrendered or extradited to the competent authorities of the issuing Member State. They shall also be deleted when the judicial decision on which the alert was based has been revoked by the competent judicial authority in accordance with national law. They shall also be deleted upon the expiry of the alert in accordance with Article 53.
2. Alerts on missing persons or vulnerable persons who need to be prevented from travelling pursuant to Article 32 shall be deleted in accordance with the following rules:
- (a) concerning missing children and children at risk of abduction, an alert shall be deleted upon:
- (i) the resolution of the case, such as when the child has been located or repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child;
 - (ii) the expiry of the alert in accordance with Article 53; or
 - (iii) a decision by the competent authority of the issuing Member State;
- (b) concerning missing adults, where no protective measures are requested, an alert shall be deleted upon:
- (i) the execution of the action to be taken, where their whereabouts are ascertained by the executing Member State;
 - (ii) the expiry of the alert in accordance with Article 53; or

- (iii) a decision by the competent authority of the issuing Member State;
- (c) concerning missing adults where protective measures are requested, an alert shall be deleted upon:
- (i) the carrying out of the action to be taken, where the person is placed under protection;
 - (ii) the expiry of the alert in accordance with Article 53; or
 - (iii) a decision by the competent authority of the issuing Member State;
- (d) concerning vulnerable persons who are of age who need to be prevented from travelling for their own protection and children who need to be prevented from travelling, an alert shall be deleted upon:
- (i) the carrying out of the action to be taken such as the person's placement under protection;
 - (ii) the expiry of the alert in accordance with Article 53; or
 - (iii) a decision by the competent authority of the issuing Member State.

Without prejudice to the national law, where a person has been institutionalised following a decision by a competent authority an alert may be retained until that person has been repatriated.

3. Alerts on persons sought for a judicial procedure pursuant to Article 34 shall be deleted upon:
- (a) the communication of the whereabouts of the person to the competent authority of the issuing Member State;
 - (b) the expiry of the alert in accordance with Article 53; or
 - (c) a decision by the competent authority of the issuing Member State.

Where the information in the communication referred to in point (a) cannot be acted upon, the SIRENE Bureau of the issuing Member State shall inform the SIRENE Bureau of the executing Member State in order to resolve the problem.

In the event of a hit where the address details were forwarded to the issuing Member State and a subsequent hit in the same executing Member State reveals the same address details, the hit shall be recorded in the executing Member State but neither the address details nor supplementary information shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing Member State shall carry out a comprehensive individual assessment of the need to retain the alert.

4. Alerts for discreet, inquiry and specific checks pursuant to Article 36, shall be deleted upon:
- (a) the expiry of the alert in accordance with Article 53; or
 - (b) a decision to delete them by the competent authority of the issuing Member State.
5. Alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38, shall be deleted upon:
- (a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between the SIRENE Bureaux concerned or the object becomes the subject of another judicial or administrative procedure;

- (b) the expiry of the alert in accordance with Article 53; or
 - (c) a decision to delete them by the competent authority of the issuing Member State.
6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted upon:
- (a) the identification of the person;
 - (b) the expiry of the alert in accordance with Article 53; or
 - (c) a decision to delete them by the competent authority of the issuing Member State.
- 6a. Alerts on persons entered by Europol pursuant to Article 37a shall be deleted upon:**
- (a) the expiry of the alert in accordance with Article 53;**
 - (b) a decision to delete them by Europol, in particular when after entering the alert Europol becomes aware that the information received under Article 37a (2) was incorrect or was communicated to Europol for unlawful purposes, or when Europol becomes aware or is informed by a Member State, that the person who is the subject of the alert no longer falls under the scope of Article 37a(2);**
 - (c) a notification, through the exchange of supplementary information, of Europol by a Member State, that it is about to enter, or has entered an alert on the person who is the subject of the alert issued by Europol;**
 - (d) a notification of Europol by a Member State participating in Regulation (EU) 2016/794 in accordance with Article 7 of that Regulation, of its reasoned objection to the alert.**
7. Where it is linked to an alert on a person, an alert on an object entered in accordance with Articles 26, 32, 34 and 36 shall be deleted when the alert on the person is deleted in accordance with this Article.

CHAPTER XV
General data processing rules

Article 56

Processing of SIS data

1. The Member States shall only process the data referred to in Article 20 for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, **37a**, 38 and 40.
2. Data shall only be copied for technical purposes, where such copying is necessary in order for the competent authorities referred to in Article 44 to carry out a direct search. This Regulation shall apply to those copies. A Member State shall not copy the 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 referred to in paragraph 2 which result in offline databases may be retained for a period not exceeding 48 hours.

Member States shall keep an up-to-date inventory of those copies, make that inventory available to their supervisory authorities, and ensure that this Regulation, in particular Article 10, is applied in respect of those copies.
4. Access to data in SIS by national competent authorities referred to in Article 44 shall only be authorised within the limits of their competence and only to duly authorised staff.
5. With regard to the alerts laid down in Articles 26, 32, 34, 36, **37a**, 38 and 40 of this Regulation, any processing of information in SIS for purposes other than those for which it was entered into SIS has to be linked with a specific case and justified by the need to prevent an imminent and serious threat to public policy and to public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the issuing Member State **or from Europol if the data was entered pursuant to Article 37a of this Regulation**, shall be obtained for this purpose.
6. Any use of SIS data which does not comply with paragraphs 1 to 5 of this Article shall be considered as misuse under the national law of each Member State and subject to penalties in accordance with Article 73.
7. Each Member State shall send to eu-LISA a list of its competent authorities which are authorised to search the data in SIS directly 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. eu-LISA shall ensure that the list is published in the Official Journal of the European Union annually. eu-LISA shall maintain a continuously updated list on its website containing changes sent by Member States between the annual publications.
8. Insofar as Union law does not lay down specific provisions, the law of each Member State shall apply to data in its N.SIS.

Article 61

Distinguishing between persons with similar characteristics

1. Where upon a new alert being entered it becomes apparent that there is already an alert in SIS on a person with the same description of identity, the SIRENE Bureau shall contact the issuing Member State **or if the alert was entered pursuant to Article 37a of this Regulation Europol**, through the exchange of supplementary information within 12 hours to cross-check whether the subjects of the two alerts are the same person.
2. Where the cross-check reveals that the subject of the new alert and the person subject to the alert already entered in SIS are indeed one and the same person, the SIRENE Bureau of the issuing Member State shall apply the procedure for entering multiple alerts referred to in Article 23. **By way of derogation, Europol shall delete the alert it has entered as referred to in point (c) of Article 55(6a).**
3. Where the outcome of the cross-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 data necessary to avoid any misidentifications.

Article 67

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

1. Data subjects shall be able to exercise the rights laid down in Articles 15, 16 and 17 of Regulation (EU) 2016/679, **and in the national provisions transposing Article 14 and Article 16 (1) and (2) of Directive (EU) 2016/680 and in Chapter IX of Regulation (EU) 2018/1725.**
2. A Member State other than the issuing Member State may provide to the data subject information concerning any of the data subject's personal data that are being processed only if it first gives the issuing Member State an opportunity to state its position. **If the personal data was entered in SIS by Europol, the Member State that received the request shall refer the request to Europol without delay, and in any case within 5 days of receipt, and Europol shall process the request in accordance with Regulation (EU) 2016/794 and Regulation (EU) 2018/1725. If Europol receives a request concerning personal data entered in SIS by a Member State, Europol shall refer the request to the alert issuing Member State without delay, and in any case within 5 days of receipt.** The communication between those Member States **and between the Member States and Europol** shall be ~~done~~ **carried out** through the exchange of supplementary information.
3. A Member State shall ~~take a decision not to provide information to the data subject, in whole or in part~~ in accordance with its national law, **including law transposing Directive (EU) 2016/680 and, in the case of personal data entered in SIS under Article 37a of this Regulation, Europol in accordance with Chapter IX of Regulation (EU) 2018/1725, shall take a decision not to provide information to the data subject, in whole or in part,** to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:
 - (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

- (c) protect public security;
- (d) protect national security; or
- (e) protect the rights and freedoms of others.

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

The Member State, **or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol**, shall document the factual or legal reasons on which the decision not to provide information to the data subject is based. That information shall be made available to the **competent** supervisory authorities.

For such cases, the data subject shall also be able to exercise his or her rights through the competent supervisory authorities.

4. Following an application for access, rectification or erasure, the Member State **or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol**, shall inform the data subject ~~as soon as possible and in any event within the deadlines referred to in Article 12(3) of Regulation (EU) 2016/679~~ about the follow-up given to the exercise of the rights under this Article **without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Member State or, in the case of personal data entered in SIS pursuant to Article 37a of this Regulation, Europol, shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall, where possible, be provided by electronic means unless otherwise requested by the data subject.**

Article 68 **Remedies**

1. Without prejudice to the provisions on remedies of Regulation (EU) 2016/679 and of Directive (EU) 2016/680, any person may bring an action before any competent **supervisory** authority ~~including~~ **or** a court, under the law of any Member State to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her.
- 2. Without prejudice to the provisions on remedies of Regulation (EU) 2018/1725, any person may lodge a complaint with the European Data Protection Supervisor in order to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her entered by Europol.**
3. The Member States **and Europol** undertake mutually to enforce final decisions handed down by the courts, ~~or~~ authorities **or bodies** referred to in paragraphs 1 **and 2** of this Article, without prejudice to Article 72.

4. Member States **and Europol** shall report annually to the European Data Protection Board on:
- (a) the number of access requests submitted to the data controller and the number of cases where access to the data was granted;
 - (b) the number of access requests submitted to the supervisory authority and the number of cases where access to the data was granted;
 - (c) the number of requests for the rectification of inaccurate data and for the erasure of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;
 - (d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the supervisory authority;
 - (e) the number of court proceedings initiated;
 - (f) the number of cases where the court ruled in favour of the applicant;
 - (g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts entered by the issuing Member State **or Europol**.

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

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

Article 72

Liability

1. Without prejudice to the right to compensation and to any liability under Regulation (EU) 2016/679, Directive (EU) 2016/680, Regulation (EU) 2018/1725 **and Regulation (EU) 2016/794**:
- (a) any person or Member State that has suffered material or non-material damage, as a result of an unlawful personal data processing operation through the use of N.SIS or any other act incompatible with this Regulation by a Member State, shall be entitled to receive compensation from that Member State; ~~and~~
 - (b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol incompatible with this Regulation shall be entitled to receive compensation from Europol;**
 - (c) any person or Member State that has suffered material or non-material damage as a result of any act by eu-LISA incompatible with this Regulation shall be entitled to receive compensation from eu-LISA.

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

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

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

CHAPTER XVIII

Final provisions

Article 74

Monitoring and statistics

1. eu-LISA 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, data quality reporting and statistics, eu-LISA shall have access to the necessary information relating to the processing operations performed in Central SIS.
3. eu-LISA shall produce daily, monthly and annual statistics showing the number of records per category of alerts, both for each Member State, **Europol** and in aggregate. eu-LISA shall also provide annual reports on the number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert, both for each Member State, **Europol** and in aggregate. The statistics produced shall not contain any personal data. The annual statistical report shall be published.
4. Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 6, 8 and 9.
5. This information shall include separate statistics on the number of searches carried out by, or on behalf of, the services in the Member States responsible for issuing vehicle registration certificates and the services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines; and aircraft, including aircraft engines; and firearms. The statistics shall also show the number of hits per category of alert.
6. eu-LISA shall provide the European Parliament, the Council, the Member States, the Commission, Europol, Eurojust, the European Border and Coast Guard Agency and the European Data Protection Supervisor with any statistical reports that it produces.

In order to monitor the implementation of Union legal acts, including for the purposes of Regulation (EU) No 1053/2013, the Commission may request that eu-LISA provide additional specific statistical reports, either on a regular or ad hoc basis, on the performance of SIS, the use of SIS and on the exchange of supplementary information.

The European Border and Coast Guard Agency may request that eu-LISA provide additional specific statistical reports for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624, either on a regular or ad hoc basis.

7. For the purpose of Article 15(4) and of paragraphs 3, 4 and 6 of this Article, eu-LISA shall store data referred to in Article 15(4) and in paragraph 3 of this Article which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/818.

eu-LISA shall allow the Commission and the bodies referred to in paragraph 6 of this Article to obtain bespoke reports and statistics. Upon request, eu-LISA shall grant access to the central repository for reporting and statistics in accordance with Article 39 of Regulation (EU) 2019/818 to Member States, the Commission, Europol, and the European Border and Coast Guard Agency.
8. Two years after the date of application of this Regulation pursuant to the first subparagraph of Article 79(5) and every two years thereafter, eu-LISA shall submit to the European Parliament and to the Council a report on the technical functioning of Central SIS and of the Communication Infrastructure, including their security, on the AFIS and on the bilateral and multilateral exchange of supplementary information between Member States. This report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify persons.
9. Three years after the date of application of this Regulation pursuant to the first subparagraph of Article 79(5) and every four years thereafter, the Commission shall carry out 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 evaluation report shall also include an assessment of the AFIS and the SIS information campaigns carried out by the Commission in accordance with Article 19.

The Commission shall transmit the evaluation report to the European Parliament and to the Council.
10. The Commission shall adopt implementing acts to lay down detailed rules on the operation of the central repository referred to in paragraph 7 of this Article and the data protection and security rules applicable to that repository. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

Article 79

Entry into force, start of operation and application

1. This Regulation shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.
2. No later than 28 December 2021 the Commission shall adopt a decision setting the date on which SIS operations start pursuant to this Regulation, after verification that the following conditions have been met:
 - (a) the implementing acts necessary for the application of this Regulation have been adopted;
 - (b) Member States have notified the Commission that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation; and

- (c) eu-LISA has notified the Commission of the successful completion of all testing activities with regard to CS-SIS and to the interaction between CS-SIS and N.SIS.
3. The Commission shall closely monitor the process of gradual fulfilment of the conditions set out in paragraph 2 and shall inform the European Parliament and the Council about the outcome of the verification referred to in that paragraph.
 4. By 28 December 2019 and every year thereafter until the decision of the Commission referred to in paragraph 2 has been taken, the Commission shall submit a report to the European Parliament and to the Council on the state of play of preparations for the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.
 5. This Regulation shall apply from the date determined in accordance with paragraph 2.

By way of derogation from the first subparagraph:

(a) Article 4(4), Article 5, Article 8(4), Article 9(1) and (5), Article 12(8), Article 15(7), Article 19, Article 20(4) and (5), Article 26(6), Article 32(9), Article 34(3), Article 36(6), Article 38(3) and (4), Article 42(5), Article 43(4), Article 54(5), Article 62(4), Article 63(6), Article 74(7) and (10), Article 75, Article 76, points (1) to (5) of Article 77, and paragraphs 3 and 4 of this Article shall apply from the date of entry into force of this Regulation;

(b) points (7) and (8) of Article 77 shall apply from 28 December 2019;

(c) point 6 of Article 77 shall apply from 28 December 2020.

6. The Commission decision referred to in paragraph 2 shall be published in the Official Journal of the European Union.

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

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

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

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

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

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Article 2
Entry into force

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

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

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament

The President

For the Council

The President