
# Report on Article 36 alerts of SIS Decision


## Executive Summary

The members of the Schengen Information System II Supervision Coordination Group ("SIS II SCG") and the Coordinated Supervision Committee ("CSC") respectively conducted a coordinated inspection activity with regard to the Schengen Information System ("SIS"). Within the scope of the inspections, the alerts and procedures with regard to Article 36 of the SIS II Decision were checked, as there has been a Europe-wide increase in the number of alerts in this alert category. In order to achieve comparable results, a questionnaire was developed by the SIS SCG and used by the Member States for their inspections.

30 data protection authorities in 19 Member States took part in the coordinated inspection activity and provided feedback regarding the questionnaire. The results indicated various differences between the Member States, enabling the CSC to draw conclusions and to recommend the necessary measures with regard to the documentation of the alerts, their quality, the time limits and retention period, as well as substantive and technical issues.

The main recommendations to the authorities initiating an alert can be summarized as follows:

- Check that all legal requirements for the alert are fulfilled.
- Check that the case and the decision to issue the alert are sufficiently documented by the responsible bodies.
- Check that all necessary data has been entered, but no information that goes beyond what is required.
- Check that necessary national procedures have been followed.

## I. Introduction

The Schengen Information System (SIS)[1] was created to counterbalance the open internal borders of the Member States of the Schengen area[2]. A second generation Schengen Information System[3] (referred to as "SIS II"), was established on the basis of the SIS II Regulation[4] and SIS II Decision[5]. This system contains alerts issued by the Member States of the Schengen area. Within the system a variety of alerts are stored, such as alerts on third-country nationals refused entry to or stay in the Schengen area and alerts on missing persons or wanted for arrest and on stolen vehicles. Up until 2023, the alerts on third-country nationals were based on the SIS II Regulation and alerts on people and objects linked to police and judicial criminal cooperation are based on the SIS II Decision.

Member States can also enter alerts for both **specific checks** and **discreet checks** in the SIS. In a **specific check,** if there is a hit on the person for whom an alert has been issued, this person is approached, checked and, if necessary, searched. In a **discreet check,** if there is a hit on the person for whom an alert has been issued, this person is observed discreetly and no arrest or check is made. Additionally, a set of data will be transmitted to the issuing authority informing about the conducted checks. From these reports, detailed profiles on movements can be generated. This type of alert is therefore linked to an intensive interference with the fundamental rights of the person concerned and sometimes even of their companions. The legal basis for this type of alert derived from Article 36 of the SIS II Decision.

In relation to this, each Member State has established a SIRENE office responsible for the quality of national data processed by the SIS. The tasks of the SIRENE Bureau are to exchange data with the Member States on alerts in the SIS II and to coordinate quality checks on the information entered in the SIS II. The SIRENE office is also competent in the area of personal data protection and deals with the issues of rights of data subjects whose personal data is recorded in the SIS. For these tasks, the SIRENE Bureau has access to the data processed in SIS.

The SIS II decision was amended and repealed by Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of

---

[1] More information can be found here: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en

[2] More information can be found here: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area_en

[3] More information can be found here: https://eur-lex.europa.eu/EN/legal-content/summary/second-generation-schengen-information-system-sis-ii.html

[4] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L 381, 28.12.2006, p. 4–23* , No longer in force, Date of end of validity: 06/03/2023; Repealed by 32018R1861. More information can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006R1987

[5] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p. 63–84, No longer in force, Date of end of validity: 06/03/2023; Repealed by 32018R1862. More information can be found here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0533

police cooperation and judicial cooperation in criminal matters.[6] Similarly to Article 36 of the SIS II Decision, Article 36 of Regulation (EU) 2018/1862 permits the competent authorities to issue alerts on persons and objects for discreet checks, or specific checks. Additionally, the new provision also allows alerts to be entered for inquiry checks.

In terms of supervision:

Until the entry into force of the new SIS related Regulations (EU) 2018/1860, 2018/1861, and 2018/1862, the supervision of SIS was coordinated among the national supervisory authorities and the European Data Protection Supervisor ("EDPS") via the SIS II SCG since the entry into force of SIS II on 9 April 2013. On 28 November 2018, the three new Regulations were adopted concerning the Schengen Information System (SIS), which entered into force on 27 December 2018. They have become fully applicable on 7 March 2023.

As a result, the coordinated supervision of the SIS II has been aligned with Article 62 of Regulation (EU) 2018/1725 ( "EU DPR")[7], that provides for an harmonised model of coordinated supervision, applicable where the relevant act of Union law refers to this Article. As per Article 62 of the EU DPR and in line with Article 69 and 71 Regulation (EU) 2018/1862, the EDPS and the national supervisory authorities, each acting within their respective competences, must cooperate actively within the framework of their responsibilities to ensure effective supervision of large-scale IT systems and of Union bodies, offices and agencies. They must meet for these purposes within the framework of the European Data Protection Board ("EDPB"). The EDPB has set up a standing Committee for this purpose, the CSC[8].

[6] 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, PE/36/2018/REV/1, OJ L 312, 7.12.2018, p. 56–106. More information can be found here: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1862. For a summary of the changes, more information can be also found here: https://eur-lex.europa.eu/EN/legal-content/summary/a-strengthened-schengen-information-system.html

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, OJ L 295, 21.11.2018, p. 39–98. More information can be found here: https://eur-lex.europa.eu/eli/reg/2018/1725/oj

[8] Coordinated Supervision Committee (CSC). More information can be found here: https://edpb.europa.eu/csc/about-csc/who-we-are-coordinated-supervision-committee_en

## II. Background

In the context of the SCG SIS II work, delegations were informed about the increase of Article 36 alerts in SIS relating to discreet and specific checks. From the statistic reports given by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ("eu-LISA")[9], it transpired that there was quite an increase on Article 36 alerts since 2013. In particular, in 2017, Article 36 alerts amounted to 129.983, resulting in 15% of the total alerts on persons in the SIS.

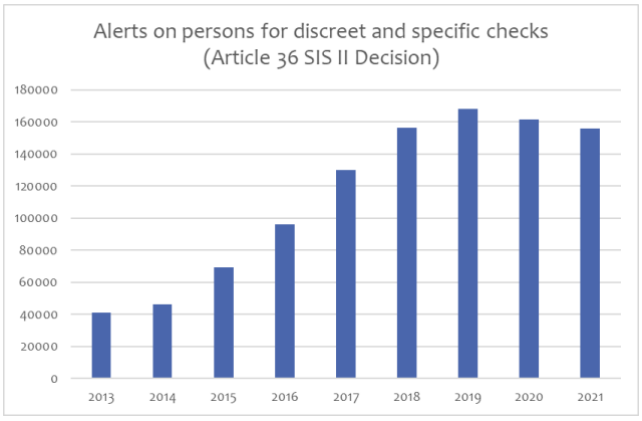


*Figure 1: Number of Article 36 alerts in the SIS II according to the public statics given by eu-LISA for the years 2013-2021*

Taking into account the abovementioned increase in alerts, the SCG SIS II decided to conduct a coordinated inspection in the Member States. This inspection involved a questionnaire prepared by the SCG SIS II and onsite checks. Previous experiences have demonstrated that these surveys can provide insight and knowledge on how the Member States implement and use those articles of the SIS Regulation and any practical problems that may occur. The purpose of the inspection was to determine, on the basis of sampling, whether the procedure and the alerts meet the requirements of the SIS II provisions. Due to the COVID-19 pandemic and related restrictions, however, few Data Protection Authorities ('DPAs') were able to conduct inspections before they stopped for almost two years. In 2022 and 2023 the DPAs resumed this activity.. The CSC succeeded the SCG SIS II for which reason the evaluation of the responses to the questionnaire is carried out by the CSC.

[9] European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) - All public available statistics on SIS can be found in the annual statistic reports on the website of eu-LISA: https://www.eulisa.europa.eu/

## III. Methodological Approach

This report builds on the replies received to the abovementioned questionnaire. In particular, the questionnaire consisted of the following three parts:

(i) questions on the number of Article 36 alerts inserted by the Member State (section 3);
(ii) a checklist (section 4); and
(iii) the assessment of DPAs from the onsite verifications (section 5).

The purpose of the questionnaire was twofold, namely to gather more specific information and statistics about the use of Article 36 alerts by competent authorities and given the nature of these alerts, for DPAs to assess the legality and the conditions under which such alerts are inserted and maintained in SIS II, in order to inform the further work of the CSC in this area.

21 responses were received from national DPAs[10]. The replies to the questionnaire provided insight and knowledge on how the Member States implement and use those articles of the SIS Regulation and any practical problems that might have occurred. The respective questions for the inspection are listed in section IV, while the findings and recommendations for possible actions to be taken by the CSC members are provided in section V of this Report.

[10] The DPAs who replied are the following: BE, BG, HR, CH, CZ, DK, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NL, NO, PL, PT, SI.

## IV. Main Findings

The results indicated various differences between the Member States, enabling the CSC to draw conclusions and recommend the necessary measures. In particular, 30 DPAs in 19 Member states[11] took part in the coordinated inspection activity and provided feedback regarding the questionnaire.

In particular, no issues were found in 12 countries out of the 19 inspected Member States and their level of compliance can be regarded as fully compliant. Improvements regarding data protection issues were considered necessary in 7 Member States.

In total, five thematic areas can be identified in which further developments are considered necessary:

1. Documentation
2. Involvement of the SIRENE Bureau and fulfilment of formal requirements
3. Time limits and retention period
4. Substantive issues
5. Technical issues

The most relevant results of the inspections in these areas are briefly described in the following:

### 1. Documentation

In accordance with Article 4 of Council Decision 2007/533/JHA (SIS Decision), SIS data is kept in a central system (Central SIS II) and, where applicable, in a national system (N.SIS II). Furthermore, the relevant authorities keep files on cases in national data systems in accordance with their national provisions. In addition to these national provisions for appropriate file management, the SIS Decision and the SIRENE Manual[12] also stipulate a certain quality of file management.

In particular, according to Article 49(1) SIS Decision, a Member State issuing an alert shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS II lawfully. In this context, Article 7(2) SIS Decision provides that the SIRENE Bureau shall coordinate the verification of the quality of the information entered in SIS II. The SIRENE Manual additionally specifies in its section 2.1.3 that the SIRENE Bureau of the contracting party issuing the alert is obliged to keep all of the information on its own alerts available to the other contracting parties. The archives of each SIRENE Bureau should be organised in such a way as to enable swift access to the relevant information in order to be able to meet very short deadlines for transmitting information. Additionally, it is explicitly mentioned that the files and other messages sent by the other contracting parties shall be stored according to procedures provided for under national law on data protection and on personal data as applicable in the receiving country.

---

[11] The DPAs taking part in the coordinated inspection activity and providing feedback on the questionnaire are the following: BE, BG, CH, CZ, DK, FR, DE (12 DPAs), GR, HU, IS, IE, IT, LV, LI, LU, NL, PL, PT, SI.

[12] Council Information: SIRENE MANUAL (2003/C 38/01) published on 17.2.2003 in *Official Journal of the European Union*, C 38/1, CELEX : 32003X0217(01).

Problems were identified regarding file management and the documentation of relevant information. The structure and content of the files kept by the competent authorities as such were criticised (e.g., the documents were not in chronological order or not kept in the relevant files). In a few cases, there was not even a full data set that could be checked initially. Consequently, in these cases it was only possible to check the documentation to a limited extent and thus ultimately the fulfilment of the substantive requirements for alerts.

At another inspection, it was not possible to determine when the alerts were entered. As a result, it was not always possible to retrieve earlier communication about an alert that had been entered and it was not possible to ascertain the background of an alert. The quality, correctness, accuracy and topicality of an alert can therefore not be guaranteed, nor can the original date of entry of an alert. This leads to the conclusion that there was a failure to comply with Article 7(2) SIS II Decision, namely to coordinate the quality control of the data entered in the SIS II and national law, because the controller has not taken sufficient measures to ensure that police data are correct and accurate in view of the purposes for which they are processed.

Another finding was that the documentation itself relating to the alerts needs to be improved. In some inspections, there was a significant lack of documentation with regard to the fulfilment of the legal requirements for the alert, the proportionality, and Schengen relevance (Article 21 SIS II Decision). Therefore, the examination of the fulfilment of the requirements of Article 36 SIS II Decision and the justification of the alert could not be sufficiently verified from the documentation in some cases. Furthermore, there were also documentation deficiencies with regard to the reviews required by the provision (e.g., regarding the necessary detailed and individual assessments in the annual review, as referred to in Article 44(4) SIS II Decision).

**2. Involvement of the SIRENE Bureau and fulfilment of formal requirements**

In each Member State, a designated authority namely the N.SIS II Office has the central responsibility for its N.SIS II according to Article 7 SIS II Decision. That authority is responsible for the smooth operation and security of the N.SIS II, shall ensure the access of the competent authorities to the SIS II and shall take the necessary measures to ensure compliance with the provisions of the SIS II Decision. Each Member State shall transmit its alerts via its N.SIS II Office.

The SIRENE Bureau of each Member State is responsible to ensure the exchange of all supplementary information in accordance with the applicable provisions. Those Bureaux have to coordinate the verification of the quality of the information entered in SIS II. For those purposes they have access to data processed in the SIS II. Beside the rules for data protection set out in the SIS Decision, detailed rules for the exchange of information are also specified in the SIRENE Manual. According to Article 49 SIS II Decision, a Member State issuing an alert is responsible for ensuring that the data are accurate, up-to-date and entered in SIS II lawfully.

The general requirements for an alert to be entered in the SIS are determined in Article 23 SIS II Decision. It is stated that a minimum amount of data is required before entering an alert. A reference is made to Article 20 SIS II Decision. This provision specifies the categories of data that can and should be entered for alerts issued in accordance with the SIS II Decision. Article 20(3) of the SIS II Decision, however, regulates that the information on persons in relation to whom an alert has been issued shall be reduced to the data mentioned therein.

In Article 21 SIS II Decision it is stated that before issuing an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II. Article 36 SIS II Decision further specifies the formal and material requirements for an alert. It is also stated that the national competent authority shall enter an alert in accordance with the national law of the Member State issuing the alert. Further specifications regarding the alert requirements can therefore be found in national provisions.

In addition to the documentation deficiencies mentioned before, a finding from the inspections was that the quality of the alerts needs to be improved in terms of the involvement of the SIRENE Bureau and the correct use of the alerts, as well as the compliance with formal requirements.

Another result of an inspection was that all of the files reviewed lacked written justification for entering an Article 36 alert. According to information obtained from the SIRENE Bureau, the SIRENE Bureau's checking of an alert is limited only to checking the necessary data to be entered. The obligation stipulated in Article 7(2) SIS II Decision, however, extends to checking also the quality of the data to be supplied before the SIRENE Bureau enters an alert. This explicitly includes quality control of the completeness of the information provided in a coordinated manner.

In some cases, the necessary case information according to Article 23(1) SISI II Decision was missing. Furthermore, it was found during inspections that the conditions required under national law were not fulfilled. Examples include cases where the necessary order authorising the alert was missing, a non-authorised person under national law had ordered the alert or relevant signatures were missing.

### 3. Time limits and retention period

In accordance with Article 44 SIS II Decision alerts on persons entered in SIS II pursuant to the SIS II Decision can be kept only for the time required to achieve the purposes for which they were entered. A Member State issuing an Article 36 alert shall, within one year of its entry into SIS II, review the need of keeping it. However, it is stated that each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

Within the review period, the Member State issuing the alert may, following a comprehensive individual assessment that needs to be recorded, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. The abovementioned one year period is also applicable in this regard. Alerts are automatically

erased after the review period of one year, except for cases in which the need for an extension of the alert has been communicated.

During the inspections of the DPAs, a number of problems were identified with regard to retention periods. For example, a finding was that the retention periods in the national files and the retention periods of the alerts were not complied with. In one case, the order to extend the time limit was not issued until after the deadline had expired. Another result was that the review periods were not adhered to.

Further, it was found that in most cases the individual assessment for the renewal of the alert was insufficient and not properly substantiated. Another finding in this regard was that the method used by the SIRENE Bureau to extend alerts does not involve a thorough individual assessment and that the alerts are renewed without prior review. In practice, this means that alerts can be extended indefinitely without the required thorough individual assessment. The extension will only be cancelled in the event of explicit rejection by the organisation. As a result, there is no review of whether the police data are still necessary for the purpose for which they were collected. This is contrary to the principle of data minimisation. In one case, the conclusion was that the data controller had not taken sufficient measures to ensure that police data are deleted or destroyed as soon as no longer necessary for the purpose for which they have been processed, or as required by any statutory provision(s).

## 4. Substantive issues

An Article 36 alert for the purposes of discreet checks or specific checks can be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) Framework Decision 2002/584/JHA. Alternatively, an alert can be issued where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future, such as the offences referred to in Article 2(2) Framework Decision 2002/584/JHA. The entry of data must be carried out by the competent national authority and in accordance with national provisions.

In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted.

In terms of violations of substantive requirements, it was observed in one inspection that police authorities issued alerts on contact persons in the SIS. With regard to alerts by police authorities pursuant to Article 36(2) SIS II Decision, the DPAs consider this to be incompatible with the wording of the European provision that refers to a person that intends to commit or is committing a serious criminal offence or will commit such a crime

in the future[13]. Even if some national laws authorise alerts on contact persons in national systems under certain conditions, such a specific legal basis is absent in the respective European law.

A further finding was that the Article 36 alert was used for a purpose other than that for which such alert is intended, namely to protect a vulnerable minor. The data subject was not the subject of an alert for the purposes of prosecuting offences or preventing threats to public safety. Improper recording of innocent persons, however, may have long-lasting adverse consequences for the data subject. Moreover, wrongful inclusion in an international police system can have far-reaching consequences for one's later life, such as when one crosses borders.

In further inspections at intelligence services, it also became apparent that the reasons for discreet checks by these authorities covered by Article 36 (3) SIS II Decision were not given in all cases. Additionally, data exchanged between national authorities after a hit was more detailed than permitted under Article 37 SIS II Decision.

## 5. Technical issues

SIS II is composed of a central system (''Central SIS II''), a national system (''N.SIS II'') in each Member State consisting of the national data systems which communicate with Central SIS II and a communication infrastructure between the two parts of the Central SIS II, the technical support function and the uniform national interface. The N.SIS II in each Member State consists of the national data systems which communicate with the Central SIS II. An N.SIS II may contain a data file (a 'national copy'), containing a complete or partial copy of the SIS II database. The communication infrastructure provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux.

According to Article 9 SIS II Decision, each Member State has to ensure the prompt and effective transmission of data. Therefore, it has to observe, when setting up its N.SIS II, the protocols and technical procedures established to ensure the compatibility of its national copy with the SIS II database and the accordance with the applicable provisions. If a Member State uses a national copy it has to ensure, by means of the services provided by the technical support function, that data stored in the national copy are identical to and consistent with the SIS II database, and that a search in its national copy produces a result equivalent to that of a search in the SIS II database.

A finding was that alerts that should have been deleted from the SIS II actually remained in that system for technical reasons, specifically for the synchronisation of the national and

[13] Article 36(2) SIS II Decision (similar wording in the corresponding provision in Art. 36(3)(a) and (c) of Regulation (EU) 2018/1862):
"2. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:
(a) where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or
(b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA."

European databases. Furthermore, there was no procedure for synchronising alerts between the national database and the SIS II information system in this case.

Another inspection result was that input data and other references are not always reliable due to migrations from other systems, the shutdown of those systems or other systemic issues. Relevant information is also lost when converting from one type of alert to another.

Furthermore, it was not possible to obtain full statistics on individual categories of information to be entered into the system. It was considered necessary to add new sections that had not been included, e.g. statistics by object category, as there is no separate accounting for objects.

## V. Considerations and Recommendations

Based on these findings, specific recommendations can be derived that are of interest to all entities issuing alerts. In this context, it is particularly important to emphasise that these findings also apply under the new legal regime, as the existing rules have been retained for the most part, although the new standards have been supplemented. As mentioned above, it is still possible for the competent authorities to issue alerts on persons and objects for discreet checks, or specific checks. Additionally, it is now possible to issue alerts on inquiry checks. Furthermore, Article 36(3) (b) Regulation (EU) 2018/1862 added another purpose enabling checks for a broader set of reasons.

Therefore, the findings of this report are interesting not only with regard to the former SIS II Decision, but also for the application of the new SIS legal framework. As it is not always possible to check every relevant aspect and at every competent authority during an inspection, the results should be of interest to all connected authorities. A harmonised use of the SIS can only be guaranteed if all competent authorities apply the rule consistently.

The DPAs recommend therefore that authorities that initiate an alert should carry out the following checks when creating an alert:

- **Check that all legal requirements for the alert are fulfilled.**
  - The adequate legal provision, under which the alert is to be inserted, should be used, in line with the requesting authority's legal tasks.
  - Authorities should not use alerts for any other purpose than that for which they are legally intended.
  - All alert requirements must always be met, in particular the requirements for ordering the alert, as well as the necessary formal requirements.

- **Check that the case and the decision to issue the alert are sufficiently documented by the responsible bodies.**
  - A chronologically and content-structured file management is the basis for working with the SIS and must be available in all cases.
  - Documentation on the fulfilment of the legal requirements, the justification, proportionality, Schengen relevance and the necessary assessments for extensions etc. must be available in a comprehensible manner for all cases.
  - If national law requires a specific order, it should be sufficiently documented that the order authorising the alert is plausible, substantiated, related to and justified by the individual case and up to date.
  - If necessary, information should be supplemented to indicate whether the alert is for preventative or repressive purposes.

- **Check that all necessary data has been entered, but no information that goes beyond what is required.**
  - Forms used by national authorities should be streamlined and mandatory, to ensure that the legal context is always given and proper justification is provided.

- **Check that necessary national procedures have been followed.**
  - The role of the SIRENE Bureau is crucial and the correct incorporation of this office with respect to data protection is essential.
  - It has to be ensured that the SIRENE Bureau always checks alerts for completeness and, if necessary, requests the organisation concerned to provide missing information without delay.
  - Some written policies are considered useful to ensure a consistent application by all officials. For instance, these policies should contain information on reviews and extensions of alert validity, deletion requirements as well supporting documents and relevant workflows.
  - If necessary, a revision of the forms in use issued by the competent authorities should be conducted.

In addition, the **extension of an alert** is an act of an authority that should only be carried out after careful consideration. This examination must be thoroughly documented together with the decisive reasons.

In the event of changes to the **technical system**, the effects on the alerts and alert categories must also be carefully assessed and any necessary amendments to the system must be undertaken. In particular, the synchronisation between N.SIS and C.SIS must function properly. The responsible bodies should take all the necessary technical and organisational measures to make all information and communication relevant to the alert transparent. It is also important to have access to useful statistics for monitoring the alerts. Sufficient categories should be created in the system for this purpose.

**Annex - Questionnaire for Article 36 alerts**

## 1. Background information

At the last meeting of the SIS II Supervision Coordination Group (SCG) delegations were informed about an article by an activist and German civil rights journal, which stressed the increase of Article 36 alerts in SIS. These alerts relate to discreet surveillance, which are generated and used without the knowledge of the individual concerned.

From the latest statistics contained in the eu-LISA report[14], it transpires that there was quite an increase (about 10% since 2013). In 2017, Article 36 alerts amounted to 129,983, which makes up 15% of the total alerts on persons in the SIS.

The group agreed to conduct a coordinated activity, which would involve a short questionnaire and an onsite check. The purpose of this exercise is twofold. The SIS SCG needs to gather more specific information and statistics about the use of Article 36 alerts by competent authorities. Furthermore, given the nature of these alerts, it is imperative for DPAs to assess the legality and the conditions under which such alerts are inserted and maintained in SIS II.

The EDPS and MT volunteered for this activity. Additional volunteers who may wish to join the activity in the process are also welcome.

## 2. Legal Framework concerning Article 36 alerts

Article 36 of the SIS II Decision[15] stipulates the following:

*"1. Data on persons or vehicles, boats, aircrafts and containers shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks or specific checks in accordance with Article 37(4).*

*2. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:*

*(a) where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or*

*(b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA.*

*3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted.*

---

[14] https://www.eulisa.europa.eu/Publications/Reports/2017%20SIS%20II%20Statistics.pdf

[15] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)- https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0533

*4. Alerts on vehicles, boats, aircrafts and containers may be issued where there is a clear indication that they are connected with the serious criminal offences referred to in paragraph 2 or the serious threats referred to in paragraph 3."*

Article 37 establishing the data categories and the action pursuant to an alert concerning discreet and specific checks, stipulates the following:

*1. For the purposes of discreet checks or specific checks, all or some of the following information shall be collected and communicated to the authority issuing the alert when border control or other police and customs checks are carried out within a Member State:*

*(a) the fact that the person for whom, or the vehicle, boat, aircraft or container, for which an alert has been issued, has been located;*
*(b) the place, time or reason for the check;*
*(c) the route and destination of the journey;*
*(d) the persons accompanying the persons concerned or the occupants of the vehicle, boat or aircraft who can reasonably be expected to be associated to the persons concerned;*

*(e) the vehicle, boat, aircraft or container used;*
*(f) objects carried;*

*(g) the circumstances under which the person or the vehicle, boat, aircraft or container was located.*
*2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.*

*3. For the collection of the information referred to in paragraph 1, Member States shall take the necessary steps not to jeopardise the discreet nature of the check.*

*4. During specific checks, persons, vehicles, boats, aircraft, containers and objects carried, may be searched in accordance with national law for the purposes referred to in Article 36. If specific checks are not authorised under the law of a Member State, they shall automatically be replaced, in that Member State, by discreet checks.*

## 3. Questionnaire

This short questionnaire is intended to gather specific information and statistics about the use of Article 36 alerts by Member States. For the purposes of this exercise, the SIS II SCG agreed to consider alerts inserted in the system since January 20XX.

3.1. How many Article 36 alerts have been inserted by your Member State since January 20XX?

3.2. Statistics on the type of alert

| Alert for / on | Person | Object connected to person |
|---|---|---|
| 36(2)(a) | | |
| 36(2)(b) | | |
| 36(3) | | |

3.3.1 Statistics by category of objects

| | |
|---|---|
| Vehicle | |
| Boat | |
| Aircraft | |

| | |
|---|---|
| Container | |

**4. Checklist**

These questions are intended to serve as a checklist for DPAs when conducting onsite verifications concerning Article 36 alerts. Depending on the volume of alerts DPAs may inspect a sample (XX%). In the case of MS generating a very small number of alerts (less than XX), the DPA shall inspect all the alerts.

This checklist is based on the specific questions concerning Article 36 contained in the Alerts Module which was adopted by the group in 2016.

For checking a specific alert:

4.1. Are the conditions of Article 36(2) or 36(3) fulfilled?

4.2. Is an alert always entered at the request of the competent authority responsible national law?

4.3. Which authorities are responsible to decide for the insertion of an alert under Article 36?

4.4. What procedures are followed for the insertion of Article 36 alerts?

4.5. What are the reasons for considering the person a threat to public security?

4.6. How long does it take to insert an alert for discreet or specific checks from the moment a person is declared a threat to public security?

4.7. What are the conditions/situations in which the alerts on specific checks are replaced by discreet checks?

4.8. When entering the alert, is all the relevant information concerning a person considered being a threat to public security available at the SIRENE Bureau?

4.9. When issuing an alert under Article 36, is the category of discreet checks or specific checks clearly indicated?

4.10. Are there procedures in place to verify that the data is complete and correctly presented? If yes, how is the information verified prior to its insertion?

For checking procedures in general:

4.11. If the information appears to be inaccurate, what action is taken?

4.12. Which authority is responsible for correcting the inaccurate data?

4.13. Which categories are entered in the system?

4.14. Are these categories in line with the minimum requisites for entering an alert in the SIS II? (Article 20 of the SIS II Decision)

4.15. In addition to the minimum data categories, is supplementary information exchanged where necessary? (vide Article 37(2))

4.16. What additional information is exchanged where necessary? (vide Article 37(1))

4.17. When entering an alert at the request of an authority responsible for national security, are all the other SIRENE Bureau informed about it by using an M form?

4.18. Is the data entered in relation to persons or vehicles, boats, aircrafts and containers for discreet checks or specific checks solely used for the purposes of prosecuting criminal offences and for the prevention of threats to public security?

4.19. Are there any other situations in which an alert for discreet checks or specific checks may be entered? If yes, under which conditions and which authorities are competent for issuing such an alert?

4.20. When supplementary information is exchanged, what are the grounds for taking this decision?

4.21. Which authorities responsible for border control or other police and customs checks (vide Article 40(1) of the SIS II Decision) have access to Article 36 alerts?

4.22. Are there other authorities having access to such information?

4.23. Are the authorities having access to SIS II included in the list which is published in the Official Journal of the European Union according to Article 46(8) of the SIS II Decision?

4.24. When collecting the information referred to in Article 37(1), are there certain conditions that must be met in order not to jeopardise the discreet nature of the check?

4.25. When a person or vehicle, boat, aircraft or container is located, what are the procedures in place to communicate such information to the issuing SIRENE Bureau?

4.26. What type of information is being communicated?

4.27. When a person or vehicle, boat, aircraft or container is not located, is there a periodic review on the necessity of maintaining the alert carried out? How often is this carried out and what are the procedures applicable?

4.28. Is there a comprehensive individual assessment on the necessity for extending the retention period of an alert on a person beyond the one year review period established under the SIS II Decision?

4.29. In the case of alerts on objects, is there a periodic assessment on the need to maintain such alerts in the system? If yes, how often is this assessment carried out?

4.30. If it results that the purposes of an alert on objects has been fulfilled, is the alert deleted prior to the expiry of the maximum retention period of five years established under the SIS II Decision? If not, what are the grounds to maintain an alert concerning objects until the expiry of such time frame?

4.31. Under which circumstances is the maximum time frame of five years extended? What considerations are made?

4.32. When the alert is deleted from the SIS II, is the data concerning the alert held in the files of the SIRENE Bureau also deleted?

4.33. If the data is not deleted, is the retention of data in the national files justifiable in view of action taken on the territory of the relevant Member State?

4.34. Where the data is retained in national files, is the maximum period of three years established under Article 47(1) of the SIS II Decision applied? Is there a longer retention period specified under national law?

4.35. When a hit occurs on an alert of Article 36, is the SIRENE Bureau of the executing Member State informing the SIRENE Bureau of the issuing Member State by using the G form?

**5. Assessment of the DPA from the onsite verifications**

5.1. How does the DPA rate the level of compliance of Article 36 alerts?

Fully Compliant _____ Partially Compliant _____ Non-compliant _____

5.2. In case of partial or non-compliance what are the reasons for this assessment?

5.3. Were there any complaints or requests for the exercise of data subjects' rights in relation to Article 36 alerts?

Number of Complaints ____
Access requests ____
Rectification requests ____
Erasure requests ____

5.4. Recommendations issued by the DPA/ future action envisaged