

**Report on logging to the SIS II at national level**

SIS II Supervision Coordination Group

# Introduction

In its work program 2016-2018, the SIS II SCG decided to carry out a study on logging to the SIS II at national level. The study aims at providing an overview of the retention period for logs, on whether the competent authorities perform log analysis and, if so, how the analysis is performed. The objective is to ensure that logs are kept and used in accordance with Article 12 as well as other data protection principles in the SIS II Decision[[1]](#footnote-1) and Regulation[[2]](#footnote-2), the SIRENE Manual and the applicable national legislation.

A questionnaire was developed to collect information at national level on the content, management, retention period and users of logs as well as on auditing and monitoring policy.

The SCG received twenty-six answers from the following Schengen States: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Norway, Portugal, Romania, Slovakia, Slovenia, Sweden and Switzerland. Two Schengen States (Cyprus and EI) replied they could not fill-in the questionnaire because their national systems were not interconnected yet.

This report first refers to the applicable legal provisions. Based on the analysis of the answers to the questionnaire, it then presents 14 findings and finally makes 18 recommendations.

# Legal background

Article 12 of the SIS II Decision and Regulation requires Member States to keep records of every access to and all exchanges of SIS II personal data for the purposes of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS II, data integrity and security (Article 12.1).

The records shall contain the history of the alerts, the data and time of the data transmission, the date used to perform a search, a reference to the data transmitted and the name of both the competent authority and the person responsible for processing the data (Article 12.3).

As regards the retention period of the logs, Article 12.4 provides for two different deadlines:

“The records may be used only for the purpose mentioned in paragraph 1 and 2 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The records which include the history of alerts shall be erased one to three years after deletion of the alerts”

The group agreed on the following understanding of Article 12.4:

* For logs of access/consultation: the retention period is of one to three years after the access occurred (to be made by all Member States/all competent authorities)
* For logs of history of the alerts (i.e. creation, alteration, deletion of the alert): the retention period is of one to three years after the alert is deleted (only to be made by the Member State introducing the alert)

Records may be kept longer if they are required for monitoring procedures that are already under way (Article 12.5).

These logs shall be accessible to the competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS II, data integrity and security, within the limits of their competence and at their request for the purpose of fulfilling their duties (Article 12.6).

# Findings

## 1. Logging

*Are the data processing activities (such as access, creation, modification, consultation, deletion) of SIS data logged? How is it managed technically? What are the actions logged?*

All Member States perform logging. Some Member States indicate that they do not provide direct access to N-SIS, so the origin of requests is a national alert management system. Hence, SIS II-related logging takes place at different stages: at the interface between the national system and the N-SIS, and at the interface between N-SIS and C-SIS.

In the case of existence of a national system distinct from the N-SIS, requests issued by the national system to the N-SIS may make use of a single, generic ID. This feature is sometimes presented positively as a way to protect the identity of agents in case of potential leaks. In this case, the N-SIS logs have to be correlated with the logs of the national system so as to determine the person at the origin of a given request.

The events logged are very diverse, some Member States indicating that above one hundred types of events can be logged. These events relate to the progress of data processing tasks taking place into the SIS II system, these tasks consisting in: creating, modification and deletion of records in the N-SIS, upload of N-SIS data to the C-SIS, download of C-SIS updates to the N-SIS, queries and access to records, etc. Extraction of data from the AFIS system is also logged.

Some Member States indicate that their logging process is transactional, so that if log recording fails, the overall transaction will fail and no data will be displayed to the user.

From a technical point of view, logging may be performed using local logging systems (the Log4J library is cited as an example) or through interconnection with a centralized logging system at the police level (Audit3 is cited as an example). All operations performed by system administrators may also be logged using a query execution management system.

In-house or third-party logging systems may implement mechanisms (such as cryptography and/or time-stamping) to enhance log integrity and its subsequent checking.

## 2. Logged items

*What mandatory data elements are logged in practice (which events and which fields for each event) ? If the Member State does not use a national copy, how is it ensured that every access to SIS II data and all exchanges of SIS II data are logged?*

The items logged are very diverse. Some Member States record the whole XML messages exchanged across the systems, while others log only some items relevant to the type of request (ID document number, car plate number, etc.). In case of update, the state of the records before and after the update may be logged, so as to determine unambiguously the nature of the modification. A Member state indicates that only information actually viewed by the user is logged.

At the application level, user authentication actions may be recorded (login / logout / unsuccessful logins), either with the national user ID and/or the SchengenID.

More specifically, depending on the Member States, the logged items may comprise:

* the whole query (without exclusion of any data), or only keywords for check activities;
* the whole answer, or else only a “hit / no hit” status, potentially including the number of hit candidates;
* timestamps of query and answer, framing the whole transaction;
* the identity of the entity performing the request (either of individual users or of the application interacting with the N-SIS in case of a generic ID);
* the location and equipment of the entity performing the request (workstation ID / session ID / SchengenID / etc.);
* the states of the transaction (e.g.: awaiting send, send in progress, N-SIS answer, C-SIS answer, as well as necessary data for resending the query in case of intermittent failure);
* contextual information (e.g.: reason for deletion).

Most logged transactions are those performed at the national level. Some Member States indicated that they do not keep tracks of actions performed by other Member States, while others capture them by logging update queries bushed by C-SIS to N-SIS.

## 3. Access to logs

*Do you have a list of the users with access to the logs and their permission to the logs?*

There is some variability among Member States on the way persons may have access to SIS II logs. Some of them distinguish several levels of access and, consequently, of authorisation: the application level and the database level.

Authorisations may be granted by the heads of respective law enforcement units, by the authorities which created the alert (SIRENE bureau), or by the national SIS office. The DPOs of these organisations, as well as the national DPA may have explicit access. Also, several other authorities have the right to request the stored data from the national logs for the fulfilment of the objectives and conditions set out in the relevant legislation: courts, prosecutor's office, national security authorities, police and investigate authorities.

Contractor personnel may be granted access on a “need to know” basis.

Several Member States impose mandatory training before granting access to logs.

## 4. Retention period

*What is the retention period of logs? How was this determined? How the retention periods are enforced (e.g. by manual deletion or an automatic one,...)?*

The duration of the retention periods varies a lot across Member States. Moreover, in some countries, the duration of the retention period depends on the type of information being logged. Member States do not have control on the logs stored in C-SIS concerning communication with the N-SIS (existence of a communication, expiration date), which may create discrepancies in log retentions. The reported durations are: 3 months (in the specific case of audit records of broadcasts and notifications, or of raw traffic logs because of their size), 1 year (sometimes only for SIRENE forms, while logs are stored longer), 2 years (plus one day or not), 800 days, 3 years (plus one month or not), 5 years or even 10 years. Non-identifying data (that is, metadata such as timestamps) may be kept even longer, for purposes of long-term monitoring of the system in terms of response time, with respect to the increase of database size and system workload.

Some of the longest durations stem from the provisions of National laws regarding police logs, that have been applied to the SIS II system as well. However, the SIS II Regulation (EC) n° 1986/2006 of the European Parliament and of the Council of 20 December 2006, provides that SIS II logs can be kept for a period of 1 to 3 years. While some Member States gave precedence of the European directive over national law, some did not, which seems in contradiction with the hierarchy of legal norms.

The rules to compute the retention period may depend on the event that generated the log. For instance, in the case of data creation, modification or deletion in the C-SIS, the retention period is computed starting from the deletion of the alert, while in the case of data transmission, it starts from the time of the query.

A majority of Member States performs an automatic deletion of the logs at the expiration of the retention period, either on a daily, monthly basis. Others perform a manual deletion, in periods of up to 6 months.

## 5. Oldest log date

*With regard to the logs showing access to SIS II data and all exchanges of SIS II data, which date is the oldest? Are the logs stored for a maximum of three years? If exceptions apply, what is the reasoning chosen?*

Answers to this question mostly refer to that of Question 4. Some Member States explicitly stated that there were no exceptions to the rules defined in Question 4, while others reported the existence of effective exceptions. These exceptions mostly relate to the preservation of data for monitoring procedures that are already under way, in compliance with Articles 12 (5). Some legal actions can delay deletion of logs, according to specific rules. A Member State declared that it could not get the information from its national law enforcement agencies.

Durations above the prescribed national retention period arise from two cases. The first one is the current lack of automatic deletion (concerning records from March 2013, April 2013) or the existence of ongoing procedures (concerning records from 1998, 2010 and 2011, related to an active monitoring task). In the case of a Member state, the oldest log date is April 2007, the date of setting-up of the system, while the oldest SIS II-related log is April 2013.

## 6. System records of log clean-up

*Do you have systems reports showing clean-up of the logs? Is there a corresponding formal procedure that these reports are part of?*

Member States which perform manual deletion do not have such records. Those which perform automatic deletion may or may not have such reports created by their system, either only at the SIS II level, or at the central level in case when a centralized logging system exists.

When created, this protocol log file may be accessible to authorised personnel of the N-SIS office.

## 7. Use of logs

*What are the logs used for?*

The majority of Member States use logs for several purposes. Only one Member state reports that its national rules of procedures stipulate that the logs are accessible only to those bodies or private persons whose duty it is to supervise compliance with the data protection regulations, and may be used only for this purpose.

The reported use of the logs are the following:

* auditing of user activities, to ascertain the lawfulness of the processing. This check can be performed by the DPA (either systematically or at the request of a data subject exercising her/his access rights), by police units (either as a check or in the course of disciplinary controls), or by judicial authorities;
* detection of abnormal activities;
* detection and investigation of security breaches;
* monitoring system performance;
* error diagnostics and troubleshooting;
* statistical purposes (for both national authorities and the EU) and future volumetric estimations. All of these do not contain any personal data.

## 8. Auditing and monitoring policy

*Do you have auditing and monitoring policy? Is this policy based on an intentionally established methodology? Please, specify the relevant standard or selected methodology.*

Some Member States do not have a formal policy, some others do have, and a few are currently in the process of designing one. The methodology is either specific to the SIS II system, or stems from existing national and/or police-related policies, including security plans. Some methodologies are based on the ITIL (“IT Infrastructure Library”) or ISKE (“IT Baseline Protection Manual”, based on a German information security standard) frameworks.

For Member States that have an explicit auditing policy, this policy may comprise up to three triggers:

* at random, possibly triggered by agents. A Member state indicates that auditing agents may take advantage of an application that displays numeric information on the activities carried out by staff members on the SIS II system;
* on a regular basis, mostly yearly for large-scale checks, or every 60 days for routine, random checks. The maximum delay between two inspections is at most 4 years, as stipulated by Article 60 (2) of decision 2007/533/JHA;
* case by case, on demand of controlling authorities.

Auditing can take the form of a paper questionnaire, followed by on-site visits that allow the inspectors to access the systems and select concrete cases at random. Automated systems are used by some Member States to help auditing agents browse through the logs.

In the case of a Member state, the lack of performing the auditing results in the locking of the account of the auditing agent herself/himself.

## 9. Regular check/inspection of logs

*Is there a regular check/inspection performed on these logs? if yes, by whom and how?*

Most Members states perform regular checks/audits. See the answers to the previous question for more details.

## 10. Automatic alerts

*Are alerts generated automatically? If yes, who monitors them or who are they sent to?*

Only a few Member States have automated alert systems. Such log-based auditing tools can be used in accordance with Article 10(1)(k) of the SIS II decision.

Security alerts are commonly processed at the infrastructure level. Alerts related to potential misuse of the SIS II system are triggered according to behavioural rules (connection outside of predetermined time slots, using another workstation than the predetermined one, etc.). Several Member States use either in-house systems, or the free/libre software Zabbix, to trigger such alerts, which are forwarded to the relevant auditing agents (national service desk and/or N-SIS team).

## 11. Who can access logs

*Who can access the logs? For what purposes?*

Partial answers to this question can also be found in answers to Questions 3 and 7.

Most Member States identify two categories of people who have access to logs:

* technical staff performing system and database administration;
* auditing staff (DPO, DPA, security staff and/or police staff).

Logs can also be accessed for the purpose of generating statistics. The statistical tool can make queries to the logs so as to generate them.

## 12. Log analysis tools

*Do you have tools to search through and analyze all the logs? Do you have tools to search through a specific type of log (DB log, application logs, system’ logs)? Are search queries possible with these tools (i.e. searching on specific fields)? Please provide details*

Partial answers to this question can also be found in answers to Question 8.

Some Member States have created and/or implemented tools to facilitate browsing through the logs. Most of these tools focus on application logs, and allow auditing agents to perform queries regarding, e.g.:

* a user in a given time interval;
* keywords (person, registration number, etc.).

The result of such queries is a display of all records containing the keywords and the personnel accessing each of these records.

Only a few tools allow to browse through system logs.

The spectrum and technicality of tools used to analyse logs is very broad:

* manual command-line queries to the database and system;
* standard Unix-like text-processing tools, e.g.: grep, awk, etc.;
* a mix of the above embedded in semi-automated, custom scripts, e.g.: SQL scripts;
* protocol-level analysis tools, e.g.: QlikView, to generate statistics;
* database-log tools, e.g.: HPE Operations Manager (to explore an unusual state of database);
* system-log tools, e.g.: HPE Operations Manager (to explore an unusual behaviour of the system), HPE ArcSlight (SIEM system – to explore possible security incidents), HPE System Insight Manager (to explore an unusual behaviour of the system), HP Open View;
* application-log tools, e.g.; Audit3, HPE Operations Manager (to explore unusual conditions of application or application server), HPE ArcSight (SIEM system – to explore possible security incidents), Oracle Weblogic Server Administration Console (to provide a detailed analysis of conditions, and possibly causes, of error messages).

## 13. Accounts and remote access

*Are logs accessed using individual accounts or using shared accounts? Are logs accessed locally or remotely via a web service or another type of service? Please provide details, including in the case of remote access details on the relevant security measures.*

Almost all Member States enforce access through individual accounts. For some Member States, however, system logs are accessed through individual accounts, while a shared account is used to provide access to application logs (to access tools such as, e.g.: Oracle SQL Developer), the query system being accessible through web services that implement individual authentication of the users.

Some Member States do not allow for remote access.

For Member States that allow for remote access, and also those which do not allow it, additional security measures may be implemented, such as:

* access is possible only through a dedicated internal network;
* access is possible only through a dedicated VPN network, using tools such as: Cisco Anyconnect, Citrix;
* access is possible only from specific IP addresses, related to specific workstations;
* special secure protocols are used (e.g.: ssh, scp, etc.);
* use of strong authentication techniques: smartcards, tokens, PIN codes.

## 14. Security measures

*Could you describe the security measures (both technical and organizational) in place to ensure the confidentiality and integrity of the logs (including from the administrators)?*

Partial answers to this question can also be found in answers to Question 13.

The set of technical security measures implemented by Member States comprises:

* connection restrictions: access from a restricted network and restricted workstations, mandatory use of cryptography and/or of a VPN, etc.;
* strong authentication methods;
* regular backups and integrity checks of logs.

The set of physical security measures comprises:

* restricted access to the premises, including e.g.: biometric authentication, CCTV, intrusion alert systems;
* physical separation of operational SIS II and auditing systems.

The set of organisational security measures comprises:

* prior security check of operators (with up to the highest clearance level);
* application of the “four-eyes” principle.

# Recommendations

In view of the findings, the SIS II SCG would make the following recommendations:

# 1) Mandatory logging

# Make sure that no data is displayed to the user unless logging has been performed (amounts to transactional logging).

# 2) Log completeness

Make sure that enough data is stored as to be able to determine exactly all the data that has been viewed/handled by the user, even in the case data is subsequently removed from the system.

# 3) Log minimization

Notwithstanding the previous recommendation, make sure that as little data as possible is stored for the aforementioned purpose.

# 4) Identity

Make sure that the identity of a user can always be ascertained. In case generic accounts are used to access the N-SIS through a national system, make sure that the actions can be traced back to individual users of the national system.

# 5) Access

Define formal access policies for all categories of persons that may have access to the system.

**6) Training**

Perform training of personnel before granting them access to logs.

**7) Retention period**

Enforce retention periods that comply with the SIS II Regulation and Decision.

Apply short periods for types of data that allow it.

# 8) Automatic deletion

Implement automatic deletion with a short period (at most monthly).

# 9) Automatic retention alerts

For data that are kept longer than the retention period (e.g. for preservation of data for monitoring procedures that are already under way), send regular alerts to assert the data is still needed (at most every 6 months).

# 10) Recording of log clean-up

Create automatic deletion reports.

# 11) Auditing and monitoring policy

Implement a formal log monitoring and auditing policy, taking advantage of existing frameworks whenever possible. This policy must provide for regular checks/audits.

# 12) Automated alerts

Implement automated auditing alert systems.

# 13) Automated browsing

Implement tools to facilitate browsing through the logs (application or system).

# 14) Remote access

In the case when remote access is available :

* perform end-to-end encryption (e.g., through a VPN); and
* strong, individual authentication.

**15) Security policy**

Implement a thorough security policy, comprising technical, physical and organisational measures.

# 16) Log integrity

The logging systems must ensure log integrity.

# 17) Log backup

Logs should also be considered in the backup policy.

# 18) Log system synchronised with C-SIS

To ensure consistency between local and central (C-SIS) logs, the logging systems should be synchronized with the C-SIS time.

Brussels, 12 June 2018

1. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *J.O.C.E*., L 205/63, 7.8.2007. [↑](#footnote-ref-1)
2. 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), *J.O.C.E.*, L 381/4, 28.12.2006. [↑](#footnote-ref-2)