EUROPEAN UNION AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE

REPORT ON THE TECHNICAL FUNCTIONING OF CENTRAL SIS II 2019-2020

MAY 2022

eu-LISA | SIS

Contents

Executive summary

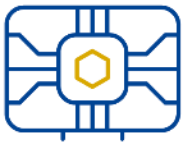
The Schengen Information System (SIS II) plays a crucial role in facilitating the free movement of people within the Schengen area by ensuring a high level of security in support of border controls at the Schengen external borders.

In 2020, SIS II's storage capacity was increased to **130 million** alerts.

2020 marked the **25th anniversary** of SIS II's entry into operation.

SIS II integration **progressed** in **Ireland** and **Cyprus** (IE connected in March 2021). The central system was made ready for the integration of **Frontex**, while **Europol** was granted extended access.

The **United Kingdom** was disconnected from SIS II on **1 January 2021** and its data was consequently deleted.



In 2020, central SIS II was available **99.94%** of the time.

SIS II was accessed **3.7 billion** times in 2020 by the Member States. Compared with 2019, the annual number of searches fell by **44%** due to travel restrictions resulting from the COVID-19 pandemic.

By the end of December 2020, according to the SIS recast regulations, all Member States were required to enable SIS–**Automated Fingerprint Identification System (AFIS)** searches at national level.

1 INTRODUCTION

1. Introduction

The Schengen Information System (SIS II) plays a crucial role in facilitating the free movement of people within the Schengen area, supporting border controls at the external Schengen borders, law enforcement and judicial cooperation, and ensuring a high level of security throughout Europe. SIS II, the key measure counterbalancing the abolition of internal border controls, has become the most widely used and largest information sharing system for security and external border management in Europe[1]. **The Schengen Information System marked the 25th anniversary of its entry into operation in 2020.**

SIS II facilitates operational cooperation between national competent authorities, including border guards, police, **SIRENE Bureaux**[2], and judicial, customs and immigration authorities. The system enables those competent authorities to enter and consult data on persons or objects, and take specific action where required. On a yearly basis, eu-LISA publishes in the Official Journal of the EU an updated list of the competent authorities having access to the system, as well as of SIRENE Bureaux[3].

Alerts on persons concern persons who may not have the right to enter or stay in the EU, wanted persons as well as missing persons, in particular children.

By the end of the reporting period (31 December 2020), SIS II was used by 30 Member States[4]; **Europol** was granted extended access to the system, while **SIS II integration had progressed in Ireland and Cyprus as well as for Frontex.**

eu-LISA (the Agency) is responsible for the operational management of central SIS II guaranteeing its effective uninterrupted access and functioning 24/7. The eu-LISA Management Board, together with the SIS II Advisory Group[5], support the Agency in this respect. eu-LISA shares responsibility for SIS II governance together with the European Commission, the Member States and several stakeholders. The Commission[6] is responsible for the correct implementation of the SIS II legal framework and any legislative initiatives linked to the system.

In December 2020, SIS II contained almost 92.5 million alerts on objects that have been stolen, misappropriated or lost.

The **SIS II Advisory Group** comprises representatives from each Member State, a representative of the Commission and appointed observers from Europol, Eurojust, and Frontex[7]. This regular forum decides on changes to be endorsed, their implementation timelines and

---

[1] SIS entered into operation in 1995 and the second generation of SIS (SIS II) has been in operation since 2013.

[2] SIRENE stands for Supplementary Information Request at the National Entries. Each EU country operating SIS has set up a national SIRENE Bureau that is responsible for any supplementary information exchange and coordination of activities connected to SIS alerts, pursuant to Article 7(2) of both the SIS II Decision and the SIS II Regulation. For more information, see: **https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation_en**

[3] OJ C 222, 2.06.2019, OJ C 188, 5.06.2020, OJ C 287, 16.07.2021.

[4] The Member States of the EU connected to SIS II as at 31 December 2020 were: Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The United Kingdom was disconnected on 1 January 2021. The Associated Countries connected to SIS II were: Iceland, Liechtenstein, Norway and Switzerland. In this document, the term 'Member States' refers to the Member States of the EU and the Associated Countries, which are bound under Union law by the legislative instruments governing SIS II.

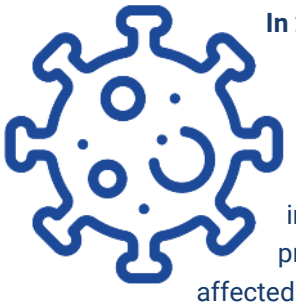
[5] The SIS II Advisory Group meets four times a year.

[6] The Commission chairs the SIS II/VIS Committee, which regularly brings together representatives of the Member States with the aim of harmonising operational procedures, supporting the effective application of the rules and optimising the use of SIS II. eu-LISA regularly reports and contributes to the committee meetings.

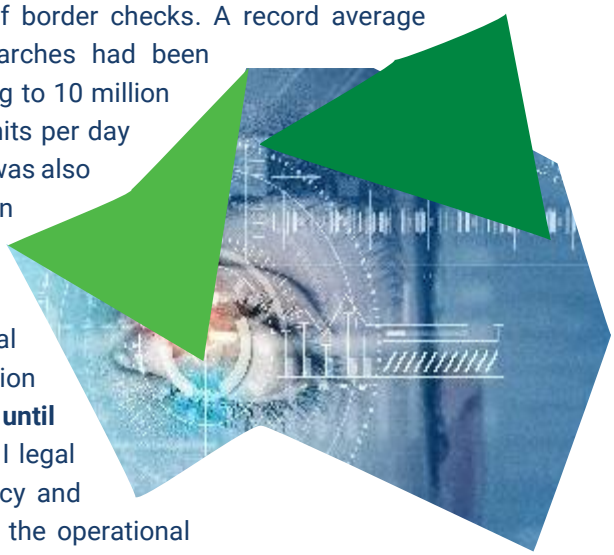
[7] Since October 2019, Frontex has attended the SIS II Advisory Group's meetings as an observer.

dependencies. The SIS II Advisory Group also reports on the availability of Central SIS II and national systems, approves release plans, discusses and plans developments, assesses training activities and validates the annual statistics.

In addition to the SIS II Advisory Group, several dedicated and ad hoc forums support the work of the Agency, including the Recast Project Management Forum (PMF), the AFIS PMF, the Security Officers Network and the National Contact Points for training.



In 2020, the number of searches and hits on SIS II dropped significantly due to the COVID-19-related travel restrictions imposed by most Member States, which led to a reduction in the number of border checks. A record average number of 18 million daily searches had been reached in 2019, before dropping to 10 million in 2020. The average number of hits per day processed by the SIRENE Bureaux was also affected in 2020, dropping by 27% in relation to 2019. However, the number of alerts stored in the system increased by 11% in 2019, and by 3% in 2020.



This report, which is the fourth report on the technical functioning of central SIS II and its communication infrastructure[8], covers the period from **1 January 2019 until 31 December 2020.** The report, as part of eu-LISA's SIS II legal reporting obligations[9], aims to increase both transparency and visibility. It encompasses activities performed to ensure the operational management of central SIS II, including its security, together with an overview of statistics collected annually.

[8] Previous issues are available on the eu-LISA website: **https://www.eulisa.europa.eu/our-publications/reports**
[9] Pursuant to Article 50(4) of the SIS II Regulation and Article 66(4) of the SIS II Decision. If not otherwise specified, in this report the 'SIS II Regulation' refers to Regulation (EC) No 1987/2006 and the 'SIS II Decision' refers to Council Decision 2007/533/JHA.

2 OPERATIONAL MANAGEMENT OF CENTRAL SIS II

2. Operational management of central SIS II

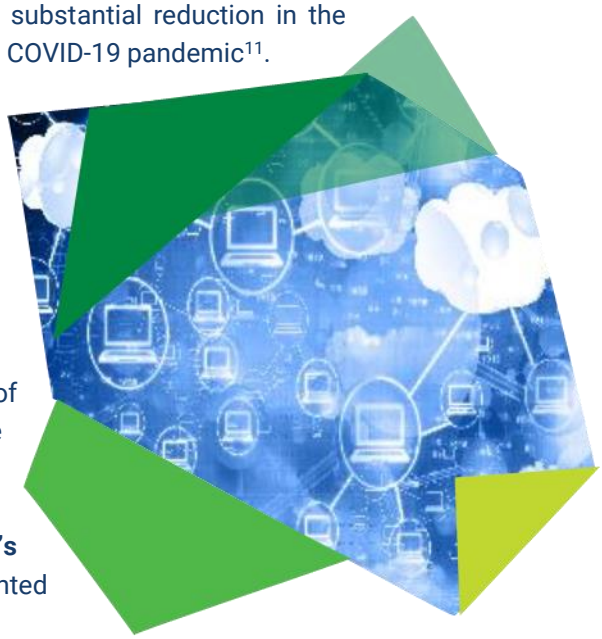
eu-LISA is responsible for the operational management of central SIS II, ensuring uninterrupted 24/7 access to the system and allowing the continuous exchange of data between the national authorities, in accordance with the legal provisions. The operational management is carried out to a large extent through management services, supervision and the implementation of appropriate corrective, adaptive and evolutionary maintenance.

External technical support was guaranteed during the reporting period by a **contractor, Sopra Steria Benelux SA/NV,** under the maintenance in working order (MWO) Single Framework Contract[10].

The MWO contract was awarded by eu-LISA following a restricted procurement procedure. **This MWO Framework Contract was concluded on 1 June 2018 for a period of four years**, with the possibility of two automatic renewals of 12 months each. By the end of December 2020, all work packages were active, including corrective maintenance, adaptive maintenance, evolutionary maintenance, as well as testing, technical assistance and training support for the Member States.

2.1 Technical infrastructure of central SIS II

In 2020, SIS II was accessed 3.7 billion times by the Member States. Compared with 2019, the annual number of searches in SIS II fell by 44%. 28 Member States reported a substantial reduction in the number of searches, as a result of the travel restrictions due to the COVID-19 pandemic[11].



The number of alerts issued by Member States and stored in the SIS II central system has grown steadily over the years, with **82.2 million alerts in 2018, 91 million in 2019, and over 93.4 million in 2020.** As in previous years, alerts on persons represented 1% of all alerts stored in SIS II. The largest categories were *Issued document,* accounting for over 71 million alerts (76%) and *Security*, accounting for over 6.5 million alerts (7%).

eu-LISA regularly carries out volumetric monitoring and analyses of central SIS II to avoid degraded service availability and to ensure that it continues to cope with increasing business needs in terms of alerts and storage of binaries, as well as searches in the central system. In this framework, eu-LISA **increased the central system's storage capacity to 130 million alerts** during 2020, which represented a major evolution of the SIS II central system.

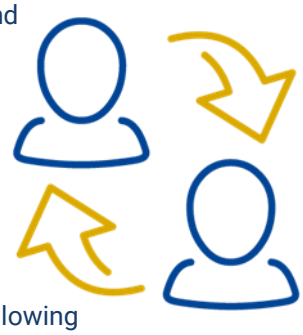
The SIS–AFIS was fully operational and maintained during the reporting period, with no major incidents. The usage of AFIS continued to increase during the same period. Once biometric fingerprint information has been added to a European Arrest Warrant, SIS–AFIS enables an even faster identification of wanted persons.

Due to the COVID-19 pandemic, various delays were experienced in the deployment of developments during 2020. In addition to supply chain disruptions, travel and access restrictions prevented the Agency's staff and contractors from working on site, e.g. for the deployment of new releases. Despite these circumstances and difficulties, the Agency made significant progress on key projects.

[10] FWC LISA/2017/RP/01 SIS II MWO.
[11] For more information, see the 2019 and 2020 annual statistical reports published on the eu-LISA website: **https://www.eulisa.europa.eu/our-publications/reports**

2.2 New SIS II users

Concerning the connection of new users to SIS II, the integration of **Ireland** progressed steadily during the reporting period. The rehearsal of the integration was performed in January 2020 and entry into operation was successfully completed in March 2021.



The integration of **Cyprus** also progressed with testing, in particular with the compliance test campaign, which was launched in April 2020. Performance and reliability testing followed during the summer and the final test report was approved at the end of 2020. As soon as the legal framework will allow, the integration project with Cyprus will be finalised and the country will be connected to SIS.

In January 2020, a release was deployed at central level containing mainly changes allowing the integration of **Frontex** as a new SIS user, as well as extended access for **Europol** as per the SIS recast regulations.

2.3 Implementation of AFIS for SIS II

In March 2018, eu-LISA implemented the Automated Fingerprint Identification System (AFIS), which introduced a biometric search capability at central level, allowing for the identification of persons of interest solely based on their fingerprints. In 2018, nine Member States (Germany, Hungary, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Portugal and Slovenia) - successfully started using AFIS. In 2019, 19 Member States were using AFIS. In 2020, six additional Member States (Bulgaria, Croatia, Denmark, Romania, Slovakia and Sweden) successfully completed testing and connected to AFIS. The connection to AFIS was a major objective for all Member States not yet connected, and eu-LISA provided them with intensive support throughout the year in this process.

By the end of December 2020, according to the SIS recast regulations, all Member States were required to enable SIS–AFIS searches at national level. By the end of 2020, 25 Member States were connected to AFIS.

SIS II AFIS Phase 2 was launched in 2019, combining the **additional biometric requirements** stemming from the SIS recast, such as the extension of search capabilities with **dactyloscopic data on palm prints and latent[12] prints** with additional performance improvements.

Following the agreement on requirements and the corresponding design for the improvement of the system's performance (September-December), the user requirements were approved by the different stakeholders by the end of 2019 and the implementation phase started in January 2020.

[12] Latent prints are impressions of fingers or palms on a surface.

This allowed the development to start as from February 2020, with the release planned in 2021. Before the end of 2020, the new AFIS hardware was delivered at the operational site in Strasbourg and a technical study was conducted ahead of its installation.

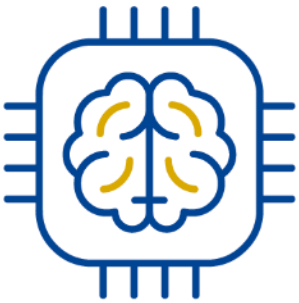
SIS II AFIS Phase 2 provides for the extension of search capabilities with dactyloscopic data on palm prints and latent prints.

2.4 SIS Recast project

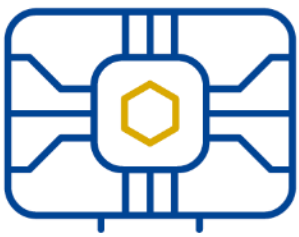
The three new regulations[13], on the establishment, operation and use of SIS II, entered into force on 28 December 2018. Their implementation has been carried out gradually since 2019 in close cooperation with the Member States and the Commission. The new system, once in operation, will represent a major enhancement, with the main changes providing for **new categories of data**[14] **and alerts**[15]**, and wider access to SIS alerts at national and European level.**

eu-LISA has been playing a crucial role in the implementation of the new regulations, being responsible for the communications infrastructure, the development of central SIS and the coordination of test campaigns with Member States. During 2019 and 2020, the Agency made significant progress on the implementation of the SIS Recast project.

In 2019, the SIS II Expert group met on a regular basis to discuss new functionalities, preferred options for implementation and their technical and operational implications for the central system. Several review cycles of the interface control document (ICD) and of the detailed technical specifications (DTS) took place until the end of 2019.



In 2020, two new features were deployed in the system. In January 2020, a new SIS II release[16] was successfully deployed in line with the new legal instruments that enable **new access control features for Europol and Frontex to query all relevant types of alerts in the system, along with fingerprint matching.** Furthermore, a search on slap fingerprints was added as an AFIS functionality that Eurojust and Frontex will be fully enabled to use once the validation and the connection of their systems is complete.



eu-LISA proceeded with the development of the two main intermediate releases of the project related to changes on alerts on persons and objects. Updated versions were also delivered for review by the Member States of the system's technical documentation, the ICD and the DTS. The updated documentation, stemming from both the AFIS and recast regulations, also covers the system's biometric elements.

[13] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals OJ L 312, 7.12.2018, p. 1; Regulation (EU) 2018/1861 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 border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 OJ L 312, 7.12.2018, p. 14; 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 OJ L 312, 7.12.2018, p. 56.

[14] i.e. biometric identifiers: fingerprints, palm prints, facial images as well as DNA concerning missing persons to confirm their identity.

[15] i.e. preventive alerts for children, alerts on return decisions and unknown persons.

[16] Release 9.3.0.

An additional stream of work was represented by the update of the Data Exchange between SIRENE Bureaux (DEBS[17]) documentation, performed by eu-LISA together with the Commission and the Member States. In December 2020, a reviewed version of the DEBS documentation was delivered. The updated DEBS documentation will ensure that the SIRENE Bureaux can exchange information on the new functionalities stemming from the SIS Recast project.

2.5 BREXIT

The United Kingdom left the European Union on 31 January 2020. At the end of the transition period which ended on 31 December 2020, the UK was disconnected from the EU large IT Systems – SIS II and Eurodac – in which it participated.

This represented a big project as it was the first time ever that a country would leave the system; in that sense everything was new. Procedures, planning and test campaigns needed to be set up and tested, bearing in mind that those should not jeopardise normal operations for the SIS community.

Prior to 31 December 2020, eu-LISA made all the necessary preparations to disconnect the UK and delete UK data from SIS II (and Eurodac). The preparations included tests and several rehearsals. By end of December 2020, over 6% of the data stored in the system was owned by the UK[18].

The process started with the technical disconnection at network level, followed by the implementation of a filter on the central system to block all UK alerts, which were then deleted. Thanks to careful planning and continuous coordination, the disconnection of the UK from SIS II did not impact the regular operations of the other Member States. **The disconnection was carried out as planned during the night of 31 December 2020, and was followed by the deletion of all UK data.**

2.6 Testing activities and releases

eu-LISA is responsible for coordinating tests, determining test requirements and planning. During the reporting period, eu-LISA supported the Member States in a variety of testing activities, ensuring the proper functioning of all systems.

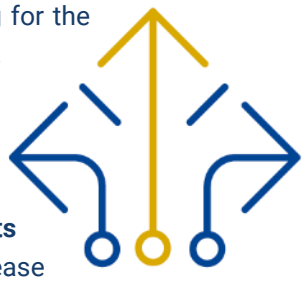
Before the deployment of each release, extensive testing campaigns are performed. The deployment and release activities are planned and performed in such a way as to minimise the impact on the operational activities of the systems, with special attention being paid to their performance and availability.

The following releases and test campaigns were deployed and performed:

- In 2019, the new ICAO 2015 transliteration rules were implemented, which represented an important business change impacting the Member States' data. Member States with high utilisation of the transliteration rules – Bulgaria, Greece and Germany – were asked to contribute to these tests. This was an important milestone for SIS II, representing the most challenging and complex enhancement of the system since its entry into operation in May 2013.

[17] A set of technical specifications defining how SIRENE Bureaux exchange information.
[18] 5 753 646 alerts.

- In January 2020, a new release was deployed[19] containing changes allowing for the integration of **Frontex** as a new SIS user and for extended access for **Europol**.



- **Europol** made preparations to set up its SIRENE office during 2020 and the office entered into operation on 8 March 2021.
- In April 2019, a project to **increase SIS II's query capacity to 130 million alerts** was launched. The project was divided into three main stages: the first release was deployed and included an upgrade of the WebLogic application software. The second release focused on the search engine, and the third release provided for an upgrade of the database. **The project continued throughout 2020,** with the first release deployed in June. However, the second release, including the implementation of the new search engine, was affected by the COVID-19 pandemic and hardware supply shortages. Therefore, although the development phase was finalised, the implementation had to be postponed to 2021.

The Agency also supported the Member States by ensuring the availability of the test and pre-production environments. From mid-March 2020, owing to the COVID-19 pandemic, **priority was given to keeping these environments highly available for the Member States** and to supporting the execution of planned testing and qualification campaigns.

2.7 Monitoring and operational activities

Central SIS II monitoring is operational 24 hours a day, 7 days a week and carried out at the operational site in Strasbourg by the eu-LISA Service Desk. The operational status of the exchange between central SIS II and the national copies (the bridge) [20] is continuously monitored. Any unavailability leading to a business impact is immediately reported and escalated on a 24/7 basis.

The eu-LISA Service Desk is the entry point for users' reports of incidents as well as for requests for information or technical advice and support. eu-LISA provides a single point contact through the Service Desk function, where users can report incidents or request a service. All requests and incidents are registered in a centralised incident management tool (SM9) for follow-up. The relevant assistance is provided based on the initial analysis, and the impact, urgency and priority are defined accordingly.

In 2019, the Service Desk handled 789 service requests and 869 incidents, of which 14 were of critical priority for SIS II. In 2020, 967 service requests and 873 incidents were processed, including 7 incidents of critical priority.

[19] Release 9.3.0.
[20] A communication infrastructure between Central SIS II and National SIS II providing an encrypted virtual network.

The main incidents were:

- In July 2019, following a switchover to the BCU[21], significantly degraded query performance was detected by the Member States and eu-LISA, causing a significant number of rejections of central queries. The Agency took the immediate decision to switch operations back to the CU[22]. The event highlighted the need for an increase in SIS II capacity, in particular in the BCU. A very large number of central queries (probably due to the holiday period) was identified as the root cause. Together with the MWO contractor, eu-LISA planned to increase available memory on BCU servers.

- In April 2020, the processing time of transactions was affected due to a message server not being available for one hour. However, no data was lost.
- On 17 September 2020, queries were fully unavailable for 40 minutes and transactions were fully unavailable for 130 minutes, due to a technical incident that affected several components of the central system. No data was lost. The troubleshooting and complete restoration of services took more than 24 hours.
- On 4 May 2020, an incident occurred on the core TESTA-ng network. No data was lost.

Central SIS II provides a data consistency check[23] (DCC) functionality to ensure the synchronisation and consistency of national copies, as well as for the restoration of data. Each month, DCC campaigns are carried out to support Member States in achieving technical compliance. Checks are performed on all alerts and links, and any discrepancies found are automatically repaired by the mechanism itself. Cases in which numerous discrepancies are found are mostly the result of incidents (and therefore lost connectivity of a given Member State with the Central system). Thanks to the regular DCC campaigns, each month all national copies are checked at least once. The results of the DCCs are regularly analysed at the AG meetings.

An increasing number of DCC campaigns have yielded no discrepancies. The share of DCC campaigns completed without discrepancies increased from 29.2% in 2018 to 34% in 2019.

In 2020, the COVID-19 pandemic had a significant impact on system usage and one of the main challenges for the Agency was to ensure the uninterrupted availability of the systems for all users 24/7. Travel and access restrictions had major implications on the staff's ability to work at the Agency's technical sites, the central unit (CU) in Strasbourg, and the backup central unit (BCU) in Sankt Johann im Pongau. Despite those difficulties, **eu-LISA managed to uphold its level of service towards the Member States, while the Agency and its staff deployed their best efforts to ensure that all systems remained available at all times.** This was a major achievement, as confirmed by the very good results in terms of system availability and response times.

As per the practice, **Member States were asked to evaluate** the eu-LISA in terms of Service Desk, Incident and Problem management, Operational Communication, Technical assistance, support for national activities and release management. The exercise is performed each year via the **Customer Satisfaction Survey,** and then presented to the AG meeting. The results from the SIS II community were very encouraging during the reporting period: in 2019, 96% of the Member States were very satisfied or satisfied (24 out of 31 stakeholders participated); in 2020, 90% were very satisfied or satisfied (28 participants).

As a follow-up, for both years, eu-LISA prepared an action plan with measures to remedy the relevant areas.

[21] Backup central unit.
[22] Central unit.
[23] The Data Consistency Check aims to support Member States in achieving technical compliance pursuant to Article 9(2) of the SIS II Decision and the parallel provision in Article 9(2) of the SIS II Regulation.

2.8 Performance and availability

When measuring performance and availability indicators for central SIS II, indicators such as **search distribution, traffic rate, maximum load and volume** should be taken into account, since the system was designed and optimised for a specific use.

SIS II was accessed 3.7 billion times in 2020 by the Member States. Compared with 2019, the annual number of searches fell by 44% because of restrictions due to the COVID-19 pandemic.

In 2019, over 28.8 million create/update/delete (CUD) transactions were performed, continuing the steadily increasing trend from the previous years. In 2020, the number of CUD operations dropped considerably to 16.5 million. During the reporting period, the majority of the transactions (98.6% in 2019 and 99.2% in 2020) were performed in less than 3 minutes, in line with the design requirements of the system.

AFIS CUD transactions have a longer Service Level Agreement (SLA) compared to alphanumerical CUD transactions. In 2019, 99.76% of AFIS CUD transactions were performed in less than 10 minutes, compared to 99.67% in 2020.

In 2019, the Member States performed more than 6.6 billion searches in SIS II, of which 10% (over 686 million) were performed in the central system. In 2020, the Member States reported 3.7 billion searches, of which 7% (267 million) were performed in the central system. As for CUD transactions, searches were also heavily impacted by the COVID-19 restrictions.

In 2019, 99.95% of all alphanumerical searches in central SIS II received a reply within the agreed time for the type of search, compared to 99.96% in 2020. Similar levels were also achieved regarding AFIS searches, with 99.94% of searches falling within the agreed SLA in 2019, and 99.88% in 2020.

Central SIS II was highly available in 2019 and 2020, confirming the trend seen in previous reporting periods. Availability is calculated based on critical SIS II functionalities, such as searching the central system or properly processing and broadcasting alerts received from the Member States. Unavailability is defined as when none of the Member States can use the critical functionalities, and it includes outages due to planned and unplanned maintenance.

In 2019, central SIS II's overall availability, including the associated connectivity network, was 99.95%. The system was unavailable for 4 hours and 1 minute. In 2020, availability was 99.94%, with the outage time amounting to 5 hours and 16 minutes in total.

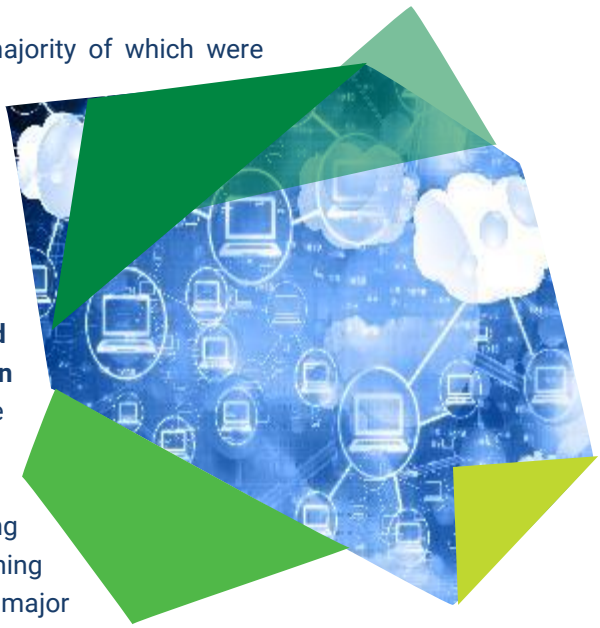
2.9 Training activities

eu-LISA is responsible for providing training on the technical use of the system to national SIS II operators, SIRENE staff and Schengen evaluators[24]. The training programme for national IT operators and technical SIS II experts facilitates the operational management of the system and supports technical maintenance; facilitates communication through the single point of contact (SPoC/Service Desk); and helps to ensure data consistency, synchronisation and data quality. In order to support new users of the system, whether Member States or Agencies, training is provided as part of the integration project connecting and supporting newcomers in developing and operating their national systems/interface.

In autumn 2019 and 2020, the **National Contact Points network for training** met to discuss and agree on training priorities, which translated into training activities for the following year. The compiled training portfolios, including the SIS II section, were provided to the network for consultation, and presented to the relevant Advisory Group at the beginning of each year.

In 2019, eu-LISA developed and strengthened its learning management system and the e-learning component of the training portfolio. **An important milestone was the development and implementation of a fully self-directed e-learning module entitled 'SIS & SIRENE Essentials'.** The training offer for SIS II included courses on SIS II for SIRENE, a series of onboarding programmes for Ireland, Cyprus, Frontex, and Europol, as well as webinars to support SIS/SIRENE Schengen evaluations.

In 2020, the COVID-19 pandemic posed specific challenges for the implementation of eu-LISA's training programme. Several years of experience in conducting online training modules facilitated the transition from face-to-face teaching to e-learning. By the end of the year, **eu-LISA's training programme included a high number of newly created e-learning products, such as online courses, e-learning modules and webinars, and an extended e-library**.



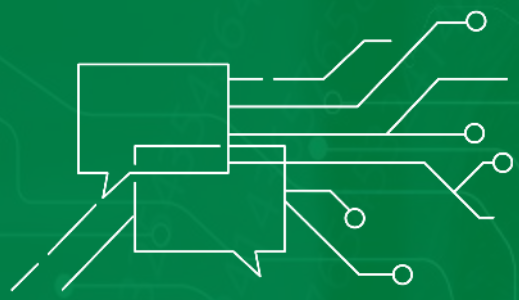
The Agency delivered **25 training sessions in 2019**, the majority of which were organised face to face, followed by webinars and new modules added to the Learning Management System (LMS). In total, **15 training sessions focused on SIS II** (i.e. 60% of the total).

Due to the COVID-19 pandemic, all but one of the **30 training activities delivered in 2020** were held online (being webinars or e-courses on the LMS). **Eight new e-learning products and training sessions were developed with a special focus on SIS II** (i.e. 27% of the total). In both years, the general average satisfaction rate was very positive[25], confirming once more the high level of appreciation for eu-LISA's profile-based training offer. The e-learning component of eu-LISA's training portfolio grew steadily until 2019 thanks to its dedicated Learning Management System (LMS) platform. However, in 2020, major efforts were made as the online platform became the main venue for training delivery. This was also reflected in the rapid increase in the number of new accounts created.

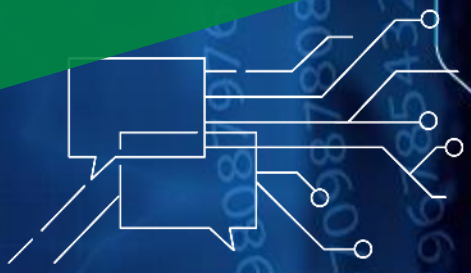
Cooperation with the Justice and Home Affairs agencies continued. As mentioned above, Europol and Frontex also benefitted from the newcomer programme with dedicated sessions.

[24] In accordance with Article 3 of the eu-LISA Regulation.
[25] On a scale from 1 to 5, the average was 4.4 in 2019 and 4.5 in 2020.

3



COMMUNICATION INFRASTRUCTURE



3. Communication Infrastructure

One of the three elements comprising SIS II is a communication infrastructure between the central system (CS-SIS) and the national system (N.SIS)[26]. The communication infrastructure provides an encrypted virtual network dedicated to SIS II data and the exchange of data between the authorities responsible for the exchange of all supplementary information (SIRENE Bureaux). **The SIS II communication infrastructure is a community under the European private secure network named Trans European Services for Telematics between Administrations — New Generation** (TESTA-ng). TESTA-ng was initially implemented by the European Commission's Directorate-General for Informatics.

The services covered by the TESTA-ng network include the provision of a Core Management Team, responsible for the overall vision, design and security of TESTA-ng and the leadership, communication and management of the service delivery team; a dedicated centralised Support and Operations Centre (SOC), responsible for ensuring the operational management by the provider and the quality of the network on a 24/7 basis; consultancy services; connectivity; network; and security. These services relate to the provision, set-up and operation of a dedicated centralised management, monitoring and support infrastructure. Additional services cover the provision of monitoring tools, reporting and SOC staffing.

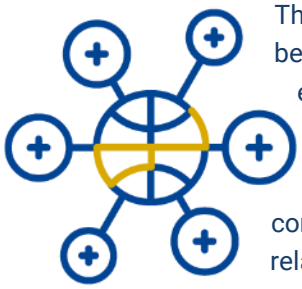
During the reporting period, the tasks regarding the communication infrastructure (including operational management and security) were divided[27] between eu-LISA and the European Commission as defined in the Memorandum of Understanding concluded in June 2014. At the end of 2018, the eu-LISA Regulation entered into force, bringing substantial changes in the management of the communication infrastructure. Under Article 11(1) of the eu-LISA Regulation, the Agency must carry out all tasks related to the communication infrastructure of the systems conferred on it by the Union legal acts governing the systems, with the exception of those systems that make use of the EuroDomain. Therefore, tasks related to the implementation of the budget, acquisition and renewal, and contractual matters relating to the communication infrastructure between the SIS II central system and national interfaces are now entrusted to the Agency.

Furthermore, Article 11(4)[28] states that tasks related to the delivery, setting up, maintenance and monitoring of the communication infrastructure may be entrusted to external private sector entities or bodies[29] in accordance with Regulation (EU, EURATOM) 2018/1046. The Agency implemented all necessary security measures in accordance with Articles 3 and 5 of the new Regulation in order to prevent external private sector entities or bodies, including network providers, from having access, by any means, to any operational data stored in the SIS II system or transferred through the communication infrastructure or to the SIS II-related SIRENE exchange.

[26] In accordance with Article 4(1)(c).
[27] The Agency was responsible for supervision, security and coordination of relations between the Member States and the network provider for the communication infrastructure of SIS II. In addition, eu-LISA was also in charge of the security measures in respect of the exchange of supplementary information through the communication infrastructure of SIS II. The Commission was responsible for all other tasks relating to the communication infrastructure, in particular tasks relating to the implementation of the budget, acquisition and renewal, and contractual matters. As regards SIS II, the Commission was also responsible for adopting the security measures, including a security plan, in relation to the communication infrastructure.
[28] Of eu-LISA Regulation
[29] All private sector entities or bodies must be bound by the security measures referred to in paragraph 3 and are to have no access, by any means, to any operational data stored in the systems or transferred through the communication infrastructure or to the SIS II-related SIRENE exchange.

3.1 Technical functioning of the Communication Infrastructure

The SIS II communication infrastructure provides a secure wide-area network for the exchange of data between central and national systems. The architecture of the SIS II communication infrastructure can be described as a 'star topology with resilience'. The CU (in Strasbourg, France) and the BCU (in Sankt Johann im Pongau, Austria) contain the central SIS II systems to which each national SIS II connects to. The CU and BCU are connected by a dedicated point-to-point connection.



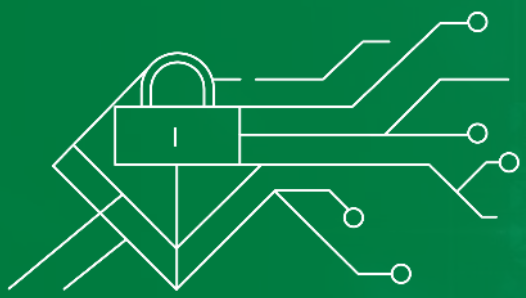
The confidentiality of SIS II communications over the TESTA-ng network, in particular between the central system and national systems, is ensured by a secondary encryption layer made up of dedicated encryption devices. These are fully managed by eu-LISA to ensure that third parties cannot gain access to clear-text data.

The SIS II-related SIRENE exchange service operates within the SIS II communication infrastructure and provides simple mail transport protocol (SMTP) relay functionality in a hub-and-spoke topology to SIRENE national systems for the purposes of supporting the SIS II-related SIRENE information exchange.

The SIS II communication infrastructure is permanently monitored to ensure continuous service availability; strict contractual performance service level requirements have been established. During the reporting period, there were no incidents with a critical impact[30] on the functioning of the overall SIS II community.

[30] A critical impact is considered to have occurred when the service is not available for more than 8 hours and the entire community is affected.

4



SECURITY & DATA PROTECTION

4. Security & data protection

4.1 Security

The SIS II security framework relies on the core principles of security; confidentiality, integrity and availability. At central level, the SIS II communication infrastructure provides assurance that the system protects the information stored and its functions as required. The SIS II central system (CS-SIS) is protected in physical terms 24/7, including a multi-layer external perimeter. Communications with Member States are protected by multiple layers of encryption and by network security controls with several layers of firewalls and integrity checks. The CS-SIS is physically located in a secure and controlled environment, isolated from the internet. Therefore, in the event of failure, operations can be switched to the backup site in Austria. Access to both systems is only granted to duly authorised persons, who hold a valid personnel security clearance and have clearly defined roles and responsibilities.

The CS-SIS must follow the security measures set out in the SIS II security plan and SIS II security policy[31], as adopted by eu-LISA's Management Board in March 2013. In 2020, the Agency carried out a risk assessment for SIS II, including AFIS. As a follow-up, new security and business continuity plans have been prepared for adoption by the Management Board in 2021.

The security policy requires, in terms of security and assessment, that **all eu-LISA systems undergo technical vulnerably tests on a regular basis**, and must provide assurance that the implementation, integration and configuration of controls are compliant with the security requirements.

Throughout the period, the Agency conducted continuous monitoring and management of residual security risks to provide assurance that the appropriate security controls for the IT systems under eu-LISA management were effective, properly implemented and managed. This included, for example, an ongoing self-assessment review of the status of eu-LISA's information security management system (ISMS).

In terms of information security, 2019 saw the introduction of a three-pronged approach to improving the security of the systems: 1) continued efforts to update and improve the Agency's security policy framework; 2) evolving the security risk management approach; and 3) consolidating the development of the technical security architecture. For example, the Agency executed a number of projects, including the implementation of the Security Information and Event Management System (SIEM) and the new Public Key Infrastructure.

Following the 2018 inspection of the European Data Protection Supervisor (EDPS) of central SIS II and the business continuity exercise carried out with the Member States, in 2019 and 2020 the Security Unit focused on the implementation of recommendations identified as part of these activities. The Agency also collaborated with the Internal Audit Service (IAS) of the Commission, which ran an IT Security audit on the large-scale IT systems within eu-LISA's remit.

Throughout 2020, preparations were made to carry out a multi-system exercise, involving the SIS II, VIS and Eurodac systems. Following common practice, the exercise involved eu-LISA and national authorities from

[31] The measures to be provided for in the security policy, according to Article 16(1) of the SIS II Decision, include restrictions on access to data processing facilities, personnel security requirements, controls on removable media containing data and any other important assets, data storage controls, passwords, access to SIS II hardware and software, communication controls for the communication infrastructure, monitoring and security incident management.

nine Member States as participants, as well as ten Member States and the Commission as observers. The exercise took place on 4 November 2020 and included a mix of cybersecurity, IT security and business continuity events within a set of pre-defined scenarios.

4.2 Data protection

The SIS II technical solution complies with strict data protection requirements at both central and national levels. **The EDPS**, in close cooperation with eu-LISA's **Data Protection Officer (DPO)**, monitors the implementation of data protection provisions, in particular concerning the processing of personal data by central SIS II.

The EDPS draft report on the inspection carried out in November 2018 on central SIS II was received in November 2019. As per the legal requirements, the eu-LISA Management Board formally adopted the comments on the report pursuant to Article 19(1)(hh) of eu-LISA's establishing Regulation for the consideration of the EDPS. The final EDPS report on the SIS II inspection was received in April 2020, containing 43 recommendations to be implemented by eu-LISA, with corresponding implementation timelines.

In order to ensure appropriate implementation of the EDPS recommendations, follow-ups were organised internally on a quarterly basis by the DPO, who proactively reported updates to the EDPS.

During the reporting period, the DPO was consulted regularly in several projects of general scope.

The SIS II Supervision Coordination Group (SCG SIS II), which brings together representatives of the national data protection authorities of the Member States and the EDPS, meets twice a year, and eu-LISA's DPO is regularly invited to report to the meetings.

The SIS II technical solution complies with strict data protection requirements at both central and national levels.

The group aims to improve cooperation between the national supervisory authorities and coordinate the supervision of central SIS II and the national systems, contributing to the exchange of relevant information and the implementation of common practices. In addition, the SCG SIS II assists national supervisory authorities during inspections and audits and provides support in the event of difficulties pertaining to the interpretation or implementation of the SIS II legal provisions.

5 SIRENE FORMS EXCHANGED & HITS REPORTED

5. SIRENE forms exchanged and hits reported

The exchange of supplementary information through SIS II contributes greatly to effective and efficient law enforcement cooperation and border management in Europe.

eu-LISA collects statistical data from the Member States on an annual basis, including data on the bilateral and multilateral exchange of supplementary information between Member States (SIRENE forms) and on hits reported.

This section presents data on SIRENE forms and hits reported by Member States for the reporting period.

5.1 Exchange of SIRENE forms

SIRENE forms are exchanged bilaterally or multilaterally between Member States (and Europol as from March 2021) in order to provide supplementary information in a structured way in relation to the data available in the system (alert).

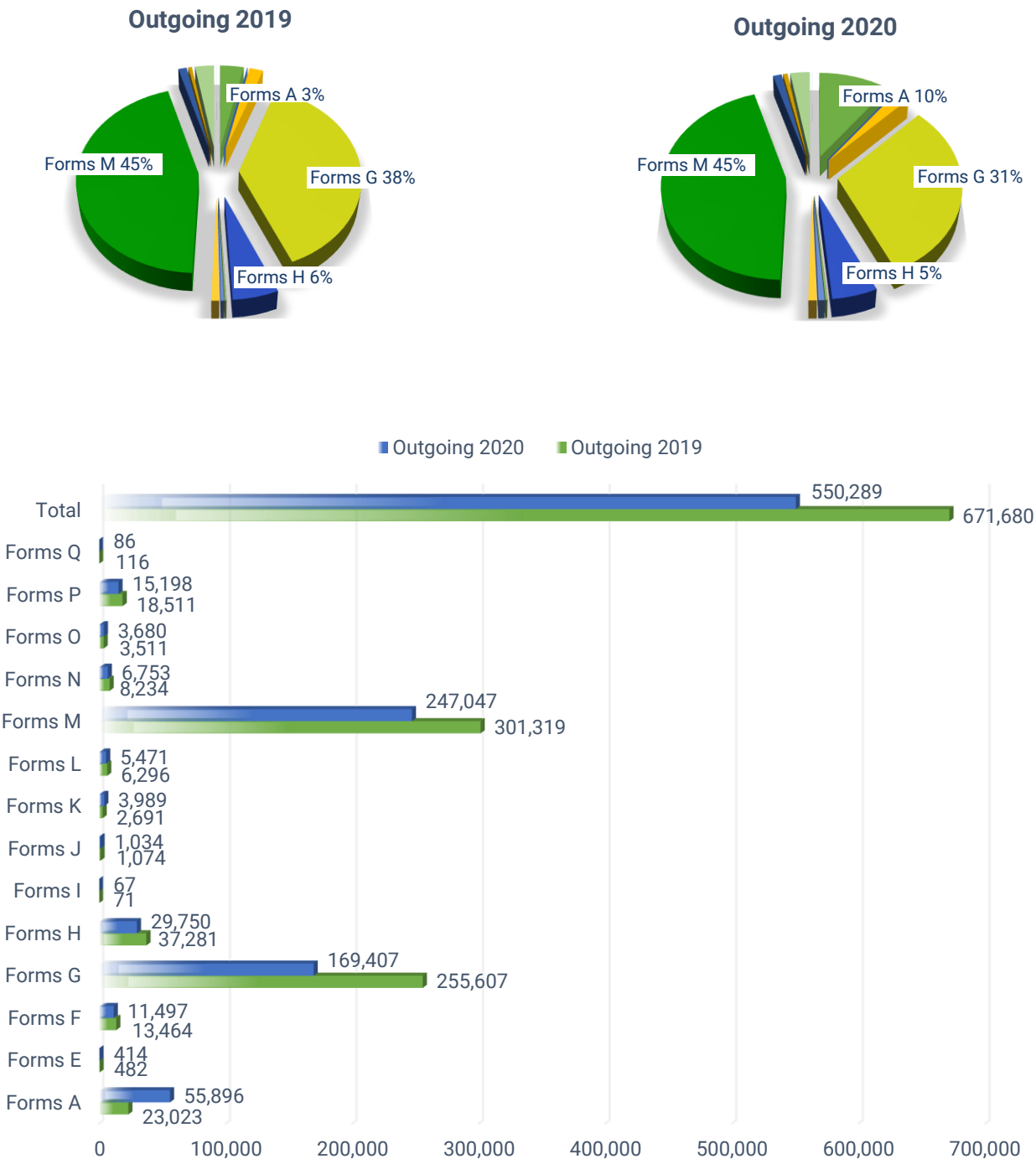
There are 14 different SIRENE forms in use; the full list is available in the SIRENE Manual[32]. The most frequently used ones are the *A Form*: supplementary information pursuant to Article 26 SIS II Decision, for European Arrest Warrant or for Extradition Request; the *G Form*: matching an alert (hit); and the *M Form*: miscellaneous information.

In 2019, there were in total **2 302 818 SIRENE forms** (671 680 outgoing forms, 1 631 138 incoming forms) exchanged bilaterally or multilaterally between the Member States. In 2020, this number fell by **14%**, with only **1 988 517 SIRENE forms** exchanged (550 289 outgoing forms, 1 438 288 incoming forms). The table and figures below provides a breakdown of outgoing and incoming forms for the reporting period.

Forms	2019		2020	
	Outgoing	Incoming	Outgoing	Incoming
Forms A	23 023	670 083	55 896	592 345
Forms E	482	498	414	698
Forms F	13 464	13 368	11 497	12 051
Forms G	255 607	244 773	169 407	172 706
Forms H	37 281	40 660	29 750	31 771
Forms I	71	82	67	68
Forms J	1 074	1 314	1 034	1 042
Forms K	2 691	2 736	3 989	4 062
Forms L	6 296	8 172	5 471	6 813
Forms M	301 319	619 077	247 047	590 616
Forms N	8 234	7 858	6 753	6 817
Forms O	3 511	3 988	3 680	3 737
Forms P	18 511	18 344	15 198	15 392
Forms Q	116	185	86	110
Total	**671 680**	**1 631 138**	**550 289**	**1 438 228**

[32] OJ L 231, 07.09.2017, p. 6.

Figure 1 — Exchange of SIRENE outgoing forms 2019 and 2020



5.2 Hits reported on foreign alerts

When a user conducts a search and the search reveals a foreign alert (i.e. the alert in SIS II matches the searched data) a 'hit' has occurred in SIS II. In accordance with the legal provisions and as a result of the hit, **further actions can be requested**.

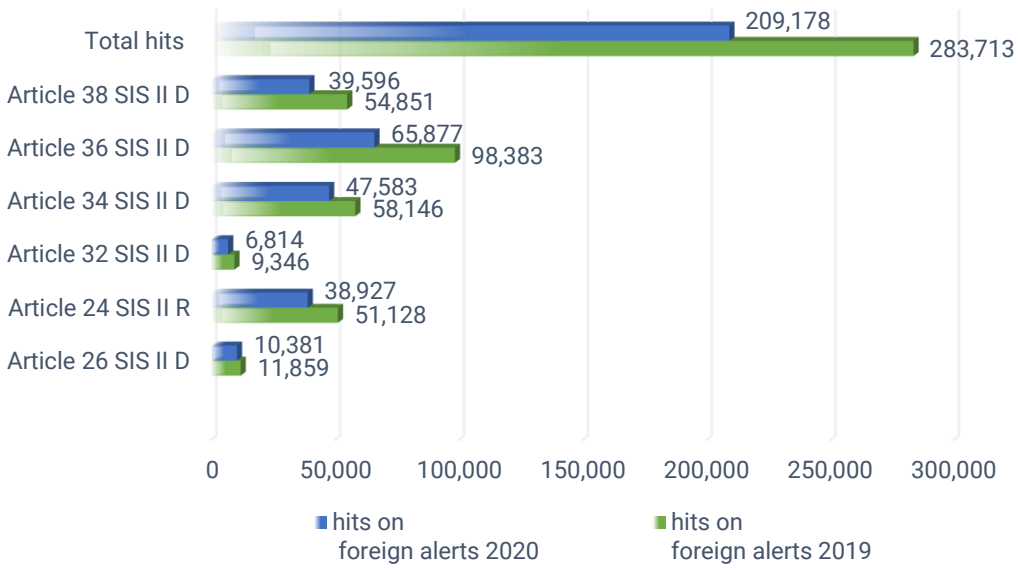
A distinction is made between hits achieved on alerts issued by other countries (i.e. hits on foreign alerts) and hits achieved by other countries on alerts issued by the reporting country (i.e. hits abroad on own alerts).

The Member States reported 283 713 hits on foreign alerts in 2019, compared with **209 178 hits in 2020,** representing a decrease of **almost 27%** between 2019 and 2020. As mentioned above, this was due to travel restrictions imposed as a result of the COVID-19 pandemic.

The table and figure below provides a breakdown of hits on foreign alerts for the reporting period.

Hits on foreign alerts	2019	2020
Hits on alerts Article 26 SIS II D	11 859	10 381
Hits on alerts Article 24 SIS II R	51 128	38 927
Hits on alerts Article 32 SIS II D	9 346	6 814
Hits on alerts Article 34 SIS II D	58 146	47 583
Hits on alerts Article 36 SIS II D	98 383	65 877
Hits on alerts Article 38 SIS II D	54 851	39 596
Total	**283 713**	**209 178**

Figure 2 — Breakdown of hits on foreign alerts reported in 2019 and 2020



Conclusions

SIS II has been **at the heart of Schengen** for over two decades, marking the **25th anniversary** of its entry into operation in 2020. SIS II plays a crucial role as the **most widely used IT system in the area of freedom, justice and security in the EU.** The system performed well during the reporting period, in line with the SLA.

The use of SIS II has steadily increased over the past years, but saw a sharp drop in the number of searches and hits in 2020 due to the COVID-19-related travel restrictions imposed by most Member States. Despite these circumstances and difficulties, the Agency has made significant progress on key projects, such as the increase in the **system's storage capacity to 130 million alerts** in 2020, and the SIS Recast project. A growing number of Member States have started using the **SIS–AFIS.**

As regards users, solid preparations were made during the reporting period for the disconnection of the United Kingdom, which was implemented on 1 January 2021. Ireland and Cyprus continued preparations in view of joining SIS II, which was achieved for **Ireland** in March 2021. In addition, the central system was made ready to connect **Frontex,** and extended access was provided to **Europol** as per the SIS Recast project.

Looking to the future, there are several major projects ahead, starting with the entry into operation of the SIS Recast project and the implementation of interoperability. Among other things, this will allow for increased effectiveness of identity checks and easier access to the systems for the relevant national authorities.

Publications Office
of the European Union

This report has been produced pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Council Decision 2007/533/JHA with the purpose of providing information on central SIS II and its communication infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.

eulisa.europa.eu

ISBN 978-92-95227-20-0

ISSN 2443-8294

doi: 10.2857/828476

Catalogue number: EL-AE-22-002-EN-N

eu-LISA | SIS