EUROPEAN
COMMISSION

Brussels, 21.12.2016
COM(2016) 880 final

# REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

## on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA

{SWD(2016) 450 final}

**REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL**

**on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Articles 59 (3) and 66 (5) of Decision 2007/533/JHA**

# 1. INTRODUCTION

## 1.1 THE SCHENGEN INFORMATION SYSTEM AND ITS ROLE IN FACILITATING THE EXCHANGE OF DATA BETWEEN MEMBER STATES

The Schengen Information System (SIS) is a centralised, large-scale information system supporting checks on persons and objects (such as travel documents and vehicles) at the external Schengen borders and reinforcing law enforcement and judicial cooperation within 29 countries throughout Europe.

SIS was established in 1995, in the six signatory Member States of the Schengen Agreement, as the major compensatory measure following the abolition of internal border controls, in accordance with the Convention Implementing the Schengen Agreement.[1] In the absence of such controls, Member States had to address the issues of cross-border crime and irregular migration. In order to maintain a high level of security, Member States had to move away from the traditional concept of bilateral agreements and legal assistance and establish a tailor-made solution to locate:

- Third-country nationals not allowed to enter the Schengen area.
- Persons to be arrested for extradition or surrender.
- Missing persons, in particular children.
- Persons and certain objects for discreet or specific checks (travelling serious criminals and threats to national security).
- Persons to assist with a judicial procedure.
- Certain categories of lost or stolen objects for seizure or use as evidence.

As a consequence, SIS was established, storing alerts on wanted persons and objects. It is directly accessible to the relevant competent authorities (see section 1.3) in the Member States, for carrying out checks and creating alerts. It includes instructions on the specific action to be taken when the person or object is located, e.g. to arrest a person, protect a vulnerable missing person or to seize an object, such as an invalid passport or stolen car. SIS underwent different evolutions throughout the years. The main ones, *i.e.* SIS 1+ and SISone4all, allowed the connection of new countries joining the Schengen area as well as enhanced technical performance.

[1] Convention Implementing the Schengen Agreement of 14 June 1985 between the Government of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders - 19 June 1990.

## 1.2 THE SECOND GENERATION OF SIS

The second generation of the system (SIS II) entered into operation on 9 April 2013.[2] The operation and use of SIS is established in two major legal instruments: Regulation (EC) No 1987/2006[3] relates to the use of SIS in checks on third-country nationals who do not fulfil the conditions for entry or stay in the Schengen area and Council Decision 2007/533/JHA[4] relates to the use of SIS for police and judicial cooperation in criminal matters.

In addition to the original features, SIS II now provides new functions and object categories:

- New categories of object alerts: stolen aircraft, boats, boat engines, containers, industrial equipment, securities and means of payment.
- The ability to conduct queries in the central system, as opposed to the previous practice of all queries being carried out in a national copy of the data.
- The possibility of linking alerts on persons and objects (e.g. alerts on a wanted person and the stolen vehicle he is using).
- Biometric data (fingerprints and photographs) to confirm the identity of a person.
- A copy of the European Arrest Warrant attached directly to alerts for persons wanted for arrest for surrender or extradition.
- Information on misused identity preventing the misidentification of the innocent party in identity fraud.

Since May 2013, eu-LISA[5] has been responsible for the operational management of Central SIS II, while Member States are responsible for the operational management of their national systems.

## 1.3 ACCESS TO SIS II ALERTS

Access to SIS II alerts is limited to the authorities responsible for border control and other police and customs checks carried out at the external borders of the Schengen area or within the relevant Member State. National judicial authorities and their coordinating authorities may also access this data.

SIS II alerts for refusal of entry or stay and blank or issued identity documents may be accessed by the authorities responsible for issuing visas and examining visa applications and those responsible for issuing residence permits and administering legislation relating to third-country nationals relating to EU *acquis* on the free movement of persons. A further access to

---

[2] The Council decided in 2001 on a second generation of the Schengen Information System which entered into operations only on 9 April 2013 for reasons set out in the Court of Auditors report of 19 May 2014 on lessons from the European Commission's development of the second generation Schengen Information system (SIS II) (http://www.eca.europa.eu/Lists/ECADocuments/SR14_03/SR14_03_EN.pdf.

[3] 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).

[4] 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).

[5] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).

SIS II for administrative purposes is granted to the vehicle registration authorities[6], who can only access alerts on stolen vehicles, number plates and vehicle registration documents.

Member States must justify an authority's access to the data in SIS. They annually provide a list of the authorities and the categories of alert to which they have access to eu-LISA for publication as required by the legal instruments. According to estimates, there are currently about two million end-users in Member States operating SIS II.

EUROPOL and EUROJUST have access to certain alert categories in SIS II reflecting their responsibilities.

### 1.4 TERRITORIAL SCOPE OF SIS II

Although SIS II is currently in operation in 29 Schengen countries, its territorial scope of application varies, as not all Member States participating in SIS fully apply the Schengen *acquis* (the collection of Schengen legislation). 26 countries fully apply the Schengen *acquis* and use SIS II for all purposes set out in the Regulation and Decision:

- 22 EU Member States: Belgium, Czech Republic, Denmark, Germany, Estonia, Greece, Spain, France, Italy, Latvia, Lithuania, Luxemburg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Slovenia, Slovakia, Finland, Sweden;
- 4 non-EU Schengen Associated Countries: Iceland, Liechtenstein, Norway and Switzerland.

*Bulgaria and Romania* currently do not yet fully apply the Schengen acquis but they operate SIS II for law enforcement cooperation. They will use SIS for external border control as soon as the decision on lifting internal border checks has entered into effect.

*Cyprus and Croatia* do not yet fully apply the Schengen acquis and it has not yet been verified that the necessary conditions for the application of all parts of the acquis have been met. They are currently carrying out preparatory activities to integrate into SIS.

Due to its partial participation in the Schengen *acquis*, the *United Kingdom* operates SIS II only within the scope of law enforcement cooperation. *Ireland* is preparing to integrate into SIS II for the purpose of law enforcement cooperation.

### 1.5 HOW THE MEMBER STATES OPERATE SIS II

In order to search the data, Member States, depending on their technical implementation of SIS II at national level, can carry out queries in either the Central SIS, in their national copy, or in both. SIS II is generally available to its end-users via their national systems. For example, law enforcement or border control authorities within a Member State will search for a wanted person or object in the relevant national databases, and in parallel, also in SIS II. In most Member States, this takes place through a single search interface. This integration into the daily working lives of end-users results in the very high use of SIS II[7]. This has brought about considerable operational success across the territories of the Member States connected to SIS II[8], all on the simple basis of making information available across national borders.

---

[6] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p.1).

[7] Section 7.2 Commission Staff Working Document.

[8] Section 7.3 Commission Staff Working Document.

The data on persons stored in SIS II is that which is necessary to locate a person and confirm his/her identity (now including a photo and fingerprints where available) as well as other relevant information about the alert (including the action to be taken). As soon as it becomes technically possible, fingerprints may also be used to *establish* the identity of a person on the basis of the biometric identifier (in the first instance, fingerprints) instead of the current use merely to *confirm* an identity. A project to introduce an automated fingerprint identification system (AFIS) to Central SIS II is in progress to facilitate this.

## 2. EVALUATION OBJECTIVES

In accordance with Regulation (EC) No 1987/2006[9] and Council Decision 2007/533/JHA[10] three years after SIS II was brought into operation on 9 April 2013, the Commission has produced a wide-ranging overall evaluation in line with the following objectives for each subject area.

### 2.1 ARTICLE 50 (5) OF REGULATION (EC) NO 1987/2006 AND ARTICLE 66 (5) OF COUNCIL DECISION 2007/533/JHA)

The evaluation targets Central SIS II; the bilateral and multilateral exchange of supplementary information between Member States; an examination of results achieved against objectives; an assessment of the continuing validity of the underlying rationale; evaluation of the application of this Decision/Regulation in respect of the Central SIS II; the security of Central SIS II and implications for future operations.

### 2.2 ARTICLE 24 (5) OF REGULATION (EC) NO 1987/2006 (ALERTS ON REFUSAL OF ENTRY OR STAY)

The evaluation targets the review of the application of this Article; making necessary proposals to modify the provisions of this Article to achieve a greater level of harmonisation of the criteria for entering alerts.

### 2.3 ARTICLE 43 OF REGULATION (EC) NO 1987/2006 AND ARTICLE 59 OF COUNCIL DECISION 2007/533/JHA (REMEDIES)

The evaluation targets the collation and review of the provisions in each Member State on: (a) a person's ability to bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him, and (b) the mutual enforcement of decisions in other Member States.

## 3. THE EVALUATION PROCESS

DG HOME carried out the evaluation internally via statistical reports, studies, questionnaires, interviews as well as in dedicated meetings and workshops.

In addition to the statistics needed for public reporting, eu-LISA collects statistics on the use of SIS II and the performance of the system itself. Member States collect statistics on the

[9] 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).

[10] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

exchange of supplementary information and hits on alerts. SIS II was designed legally and technically from the outset to provide statistics on its use and effectiveness.

On the technical and operational management aspects of SIS II, the report described in Article 66(4) of the SIS II Decision and provided by eu-LISA was incorporated into the overall evaluation[11]. This report describes the technical functioning of Central SIS II and the network, including the security thereof, from the entry into operation on 9 April 2013 until 31 December 2014. Looking to the future, to identify solutions for a range of technical issues raised by the Member States, the Commission initiated a study[12] on possible improvements to the SIS II architecture in order to seek cost efficiencies, improve business continuity, handle increased use of the system and the different types of transactions that will be needed, especially fingerprints.

The security of Central SIS II was assessed through incorporation of the eu-LISA report on Central SIS II and relevant sections from the 2014 European Data Protection Supervisor audit of Central SIS[13].

The evaluation continued with open questions on the technical and operational aspects of the SIS II. The questions covered operational and legal issues but the responses were also assessed and presented in terms of the five key evaluation criteria: effectiveness, efficiency, coherence, relevance and EU added-value.

In order to collect data to help evaluate the use of alerts on refusal of entry or stay and the consultation procedures, a series of questions was addressed to the Member States via the Commission-chaired European Migration Network.

The sections on bilateral and multilateral exchange of information, the examination of results and implications for future operations and the assessment of the continuing validity of the underlying rationale were completed using statistical analysis, questionnaires to key stakeholders and discussion at face-to-face meetings with the national police authorities.

The section on remedies contains the key points of the report provided by the SIS II Supervision Coordination Group and the information gleaned from a targeted questionnaire. Detailed questions on specific areas were forwarded to the national contact points.

The extensive evaluation evidence was summarised in a Commission Staff Working Document. This report contains references throughout to the more detailed information contained within the Staff Working Document.

## 4. FINDINGS OF THE EVALUATION

### 4.1 INTRODUCTION TO THE KEY FINDINGS

SIS II is an operational system which cannot remain static and has demonstrated obvious success against a background of evolving and complex issues. Accordingly, the evaluation not

[11] eu-LISA's technical report on the functioning of Central SIS II http://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20Technical%20Report%202015.pdf

[12] European Commission FINAL REPORT — ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016.

[13] Report on inspection pursuant Article 47(2) of Regulation (EC) N. 45/2001 on the Schengen Information System II (SIS II) managed by the EU Agency for large-scale IT systems (eu-LISA) case reference: 2014-0953.

only examined existing performance but also looked to the future to propose major evolutions in technology, managing workload, protecting individual rights and achieving better operational outcomes.

Notwithstanding the considerable success and EU added-value achieved through the use of SIS II and its ongoing relevance to the serious security and migration challenges faced by Europe, the Commission has identified certain points to be addressed. The numerous points range from technical detail to potential changes to the legal instruments and therefore this document will provide a broad overview.

### 4.2 HAS SIS II ACHIEVED ITS OBJECTIVES IN BRINGING EU ADDED VALUE?

#### 4.2.1 Outcomes concerning the use of SIS II

This section gives an overview of the results achieved through the Member States' use of SIS II and subsequent cooperation via the SIRENE Bureaux since the entry into operations. This sheer volume of positive outcomes could simply not have been envisaged through bilateral cooperation. The competent authorities checked persons and objects against data held in SIS II on nearly 2.9 billion occasions in 2015 alone. At present, the system contains over 69 million alerts. In order to create, update or delete alerts on persons or objects or to extend the lifetime of an alert, a further 20.7 million transactions took place in 2015.

A 'hit' in SIS II means that the person or object has been found in another Member State and further action, specified in the alert, is requested. Between the entry into operation of SIS II on 9 April 2013 and the end of 2015 **over 371 000 hits** were achieved (an average of over 370 hits per day).

This equates to:

- Over 25 000 people arrested to face justice in another Member State.
- Over 79 000 people refused entry or stay in the Schengen area (having already been subject of a decision on refusal of entry or stay).
- Over 12 000 missing persons found having crossed a border into another Member State.
- Over 83 000 people traced to assist with a criminal judicial procedure. Where the alert has been created by the police on behalf of the judicial authorities, following a hit, there is an ongoing issue of the alert not being deleted in a timely fashion.
- Over 72 000 travelling serious criminals and other people posing threats to security located.
- Over 97 000 cases solved concerning stolen motor vehicles, misuse of identity or travel documents, stolen firearms, stolen number plates and other lost or stolen property. However, low levels of success were noted in the categories banknotes, securities and means of payment, despite a high number of alerts.

Furthermore, all the alert categories described above have seen steady increases in hits. In the single year 2014-15 SIS end-users achieved:

- 27 % increase in arrests for extradition or surrender.
- 18 % increase in locating people for refusal of entry or stay in the Schengen area.
- 44 % increase in finding missing persons.
- 10 % increase in tracing people to assist with a criminal judicial procedure.

- 43 % increase in locating travelling serious criminals and people posing threats to security.
- 18 % increase in solving cases concerning stolen motor vehicles, misuse of identity or travel documents, stolen firearms, stolen number plates and other lost or stolen property[14].

### 4.2.2 The SIRENE Bureaux

Amongst all forms of European law enforcement cooperation, communication related to SIS II alerts is by far the largest. SIS II stores sufficient data for front-line officers to identify a person or an object when he/she achieves a 'hit' on an alert. There is, however, another need for Member States to consult each other about the circumstances of the specific case and this communication is carried out by the SIRENE Bureaux[15]. Every country that operates SIS II has a SIRENE Bureau, established as a single national contact point for communication on SIS II alerts. These SIRENE Bureaux provide any necessary supplementary information on alerts and coordinate activities in relation to the alerts; generally through the use of structured electronic 'forms', using strictly regulated procedures and a secure, dedicated computer network.

In 2015, just over 1.8 million forms were sent or received by the SIRENE Bureaux[16], an increase of 27 % from 2014. SIRENE Bureaux are also responsible for data quality and coordination of cross-border operations.

The SIRENE Bureaux are at the very heart of SIS operation and play a key role in effective information exchange. Their effectiveness is increased by ongoing training programmes at national and European levels. The operation of the SIRENE Bureaux serves as a model for other law enforcement communication channels.

Appropriate staffing levels and sufficient technical support are necessary to enable the SIRENE Bureaux to effectively carry out the bilateral and multilateral exchange of supplementary information between Member States, to communicate on hits and to handle the necessary procedures within the legal time-limit required (normally 12 hours, however in the case of discreet and specific check alerts requiring immediate reporting, this must be done immediately). The evaluation noted a significant increase in the exchange of forms, due to a rise in hits and the extensive use of discreet and specific check alerts, especially with respect to terrorism-related activities. Whilst the number of exchanged forms substantially increased in 2015, staffing levels at SIRENE Bureaux remained unchanged. This forced certain Member States to prioritise their work and disregard the mandatory 12-hour response time, which has brought several SIRENE Bureaux to the limits of efficient operation[17].

### 4.2.3 Conclusion

Subject to further detailed work with the Member States on refining the use of some alerts on objects where there is either little usage or little success, or where deletion of the alert is not carried out in a timely manner, the Commission's overall conclusion is that the underlying rationale for SIS continues to be valid. There is very strong evidence of the achievement of results (hits) against stated objectives (alerts).

---

[14] Section 7 Commission Staff Working Document.

[15] SIRENE stands for Supplementary Information Request at the National Entry.

[16] Information can be sent bilaterally or multilaterally. As each SIRENE 'form' represents a task for both sender and recipient, when measuring workload both forms sent and received are counted.

[17] Sections 12.2; 17.4 Commission Staff Working Document.

SIS II constitutes significant EU added value, as cross-border law enforcement cooperation in such high volumes could not take place without this database. No other law enforcement cooperation system generates as many positive outcomes or can handle as much information flow in real time with the result that, year on year, in all alert categories, hits have increased.

### 4.3 HAS SIS II ACHIEVED ITS OBJECTIVES IN AN EFFECTIVE WAY AND CAN IT MEET NEW CHALLENGES?

The underlying principle of SIS II is that information is made available to end-users, with clear instructions on what to do and where to go for round-the-clock support (SIRENE Bureaux). The Commission's view is that the concept is highly effective.

In order to maintain this level of effectiveness the Commission has identified both strategic and detailed findings requiring attention and improvement in technical, organisational and operational spheres. For the purposes of this report and to maintain conciseness, these findings are summarised under generic themes.

#### 4.3.1 SIS II must remain a flexible system, capable of swiftly addressing new operational phenomena

The SIS II legal instruments set the framework requirements for SIS II and the principles of its operation; the detailed procedures, however, are laid down in implementing rules[18]. This provides a flexible framework which has already allowed effective legal and technical interventions to enhance information exchange, in particular on travelling terrorist suspects and sexual offenders. Complexity emerges, however, in the change management process, as technical changes must often also be integrated into the national law enforcement or immigration systems.

In conclusion, although the very swift implementation of changes related to terrorism was a considerable success, it is clear that, for future changes, technical, financial and contractual resources must be made available at central and national levels to be able to handle the process in a more rapid and effective manner[19].

#### 4.3.2 Business continuity must be further improved

The technical architecture of SIS II gives flexibility to Member States to have their own national copy or to use Central SIS II[20] for queries. Five Member States, not having national copies, face the serious risk that if the network connection breaks down or Central SIS II becomes unavailable, they do not have a fall-back option and so access to SIS II alerts would be completely interrupted. Member States with a national copy should also ensure appropriate business continuity solutions, either by having a back-up system or by allowing their end-users to search Central SIS II directly.

In conclusion, business continuity must be ensured at central level and downtime of Central SIS II should be avoided. Technical solutions will be explored to decrease the switchover time

[18] Such as the Commission Implementing Decision (EU) 2016/1209 of 12 July 2016 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2016) 4283) (OJ L 201, 28.07.2016, p.35) and in technical documentation (Detailed Technical Specifications and the Interface Control Document).

[19] Section 6.2.1 Commission Staff Working Document.

[20] CS-SIS is the technical support function containing the Central SIS II database.

between Central SIS II and its back-up site as the current technical possibilities and procedures are not considered to meet the expected standards on system availability.[21]

### 4.3.3 SIS II is not always queried automatically when the national system is queried but an additional transaction by the end-user is required

Even though SIS II was accessed by the competent authorities 2.9 billion times in 2015, one billion times more than in 2014, the use is uneven. Annual statistics show that certain Member States and Member States' authorities do not query SIS II systematically when they query their national police or immigration databases, which means that they need to search SIS separately with an additional transaction which does not always happen.

In conclusion, taking into account that crime has gained an increasingly European dimension, Member States must ensure that every time they check their national databases they also include a parallel check in SIS II[22]. The Commission will ensure that the Schengen evaluation mechanism focuses on this issue.

### 4.3.4 Checking SIS II at the external borders

The Schengen Borders Code[23] imposes an obligation to verify, in particular by consulting SIS II, that third-country nationals entering the Schengen area '*are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States*'[24]. In some Member States border guards do not check the travel documents of all third-country nationals against the databases at airports. In some Member States it was observed that the border guards did not check all third-country nationals systematically but employed risk assessments. Only the checks against SIS II of EU citizens entering the EU should be based on a risk assessment[25] [26] [27]. In other cases technical failures of the applications used by border guards can lead to the non-satisfactory checks in SIS II.

In conclusion, Member States must sufficiently check SIS II at the external borders in line with legal expectations. The Commission will ensure that the Schengen evaluation mechanism focuses on this issue.

### 4.3.5 New categories of alert or the new functionalities (fingerprints, photographs, European Arrest Warrant, links, misused identity extension) are not fully implemented and displayed to the end-users, contrary to the SIS II legal instruments[28]

This shortcoming diminishes the effectiveness of the system since the end-users are not able to establish all the circumstances of the case and might even miss essential information.

---

[21] Section 6.2.1 Commission Staff Working Document.

[22] Section 6.2 Commission Staff Working Document.

[23] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

[24] Article 8 (3) (a) (vi) of Regulation (EU) 2016/399.

[25] According to the currently applicable provisions of the Schengen Borders Code [Article 8 (2)].

[26] The Commission nevertheless adopted on 15 December 2015 a proposal as regards the reinforcement of checks against relevant databases at external borders. This proposal provides in particular for a systematic check of individuals enjoying the right of free movement against the SIS II (COM(2015) 670 final).

[27] Sections 15.1 and 16.1 of Commission Staff Working Document.

[28] Parallel Articles 3 (a) and (c) read in conjunction with Articles 20 (3) of Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA.

Officers lose time by having to contact the SIRENE Bureau for the missing information. In many cases they do not have the right to detain the person subject to the alert and yet cannot properly identify him/her. Some Member States cannot add photographs and fingerprints to their alerts[29].

In addition, given the rise in the use of false identities, in order to be able to move from the current situation where fingerprints are only used to confirm the identity of a person, to a situation where the identity of a person can be revealed solely from his fingerprints, the planned automated fingerprint identification functionality should be added to SIS II with all due speed[30].

In conclusion, the Commission will put forward a proposal to ensure that all appropriate functionalities are made available to the end-users.

### 4.3.6 Poor data quality is a major issue for the use of SIS II

When creating alerts, Member States sometimes enter incorrect or incomplete data (for instance, an incomplete name or a name instead of a document number). The consequence of entering low quality data is that queries performed in the system may not locate the person or object or the person cannot be properly identified on the basis of such data. According to the SIS II legal instruments, Member States are responsible for data quality[31]. Member States are therefore required to establish an effective mechanism at national level for data quality controls but they have not all yet done so.

The Commission will also seek to formalise the role of eu-LISA in highlighting common data quality problems.

### 4.3.7 Many Member States have not implemented all search combinations provided in Central SIS II

Many Member States use 'exact match' queries (no fuzzy or partial query). Sometimes, this is due to national data protection legislation which requires Member States to always enter first name, surname and date of birth to carry out a query on a person. (This is the case in two Member States). Therefore, some Member States are not able to find alerts where the first name or the date of birth is missing or incomplete. A similar problem applies to some queries for objects. In one Member State, end-users can only query on objects with exact parameters. This means that they will miss alerts where the recovered object's identification number is not clear or attempts have been made to obliterate it[32].

The Commission will also put forward a proposal to ensure that the full query tool capability of Central SIS II is replicated at the national level.

### 4.3.8 In certain Member States end-users cannot use SIS II to its full capacity

This situation can occur when one or more of the following criteria are missing:

- clear instruction for end-users on their screen on the action to be taken;
- mandatory post-hit procedures, including the reporting of hits, and

[29] Section 16.1 Commission Staff Working Document.
[30] Section 6.1; 6.2.1; 6.2.2; 13.1; 14.1 Commission Staff Working Document.
[31] Article 34 (1) of Regulation (EC) No 1987/2006 and Article 49 (1) of Council Decision 2007/533/JHA.
[32] Section 16 Commission Staff Working Document.

- sufficient training on the use of the system[33].

In conclusion, the Commission will ensure that the Schengen evaluation mechanism focuses on the implementation of appropriate instructions, procedures and training.

### 4.3.9 Limitations to the effectiveness of SIS II in combatting illegal immigration

Alerts for the refusal of entry or stay are issued for third-country nationals who are not allowed to enter or stay in the Schengen area following a decision by a competent national court or authority. The evaluation demonstrated that there are situations in which a Member State may decide to grant a person the right to enter into or stay on its territory despite the existence of a refusal of entry alert issued by another Member State, and even where no legal exception applies. As a consequence, the EU-wide effect of such alerts is not systematically achieved. In addition, Member States reported shortcomings in the processes and quality of information-exchange concerning these alerts, especially in the context of the related consultation procedure[34].

It is clear that both the lack of harmonisation in consultation and tardy responses cause operational staff and the individual concerned considerable problems.

The evaluation highlighted that under this alert category, the overall number of cases when the requested action cannot be taken, i.e. to refuse the entry or stay, is the highest amongst all alert categories in SIS II[35]. SIS II is effectively 'identifying and finding' the alert subjects but the different and often confusing interpretations of the legal provisions on entry bans and residence permits undermine its efficiency and effectiveness at EU level, resulting in incoherence.

In conclusion, the Commission will put forward proposals on the harmonisation of procedures related to alerts for refusal of entry or stay.

### 4.3.10 The rules on data protection in the legal base need to be reviewed in order to reflect recent EU data protection reform[36]

At the level of implementation, the evaluation shows that effective mechanisms are in place in Member States for the data subjects to access, correct, delete their personal data in SIS II or obtain compensation in connection with inaccurate data. However, there is a lack of standardised information regarding remedies at national level. Although the procedures to obtain remedies can include the activities of the data controller and the supervisory authority it especially pertains to the courts, where it is difficult to obtain information on the number of requests for recourse.

Other areas to be improved include procedures and documentation related to data security - in line with recommendations from the audit carried out by the European Data Protection

[33] Section 17.3 Commission Staff Working Document.

[34] Pursuant to Article 25 (2) of Regulation (EC) No 1987/2006, where there is a hit for refusal of entry or stay on a third-country national who is beneficiary of the right of free movement, the Member State executing the alert should consult immediately the issuing member State through its SIRENE Bureau in order to decide on the action to be taken.

[35] Section 7.2 of the Commission Staff Working Document.

[36] (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016).

Supervisor - and data quality, including measures at the level of Central SIS II and harmonisation of national practices.[37]

Moreover, the wording of the legal instruments will be reviewed so that it reflects the new EU data protection legislative framework[38]. The Commission will propose amendments to the legal instrument to require the development of a standardised annual statistics package. This will allow consistent reporting on activities on remedies at national level, including the activities of the data controller, the supervisory authority and the courts. Additionally, the Commission will scrutinise eu-LISA's response to its security audit.

### 4.3.11 Security of Central SIS II is provided effectively[39]

The Commission asked eu-LISA to provide a detailed breakdown of the most critical network incidents affecting SIS II availability since its entry into operation. It was shown that there have been no incidents where data at the central level were at risk of compromise.

In conclusion, subject to detailed procedural findings in the security audit, the overall conclusion on the security of Central SIS II is that it is highly effective.

## 4.4 IS SIS II COHERENT WITH OTHER PIECES OF RELEVANT EU LEGISLATION?

SIS II can only be effective if it works in synergy with all instruments supporting law enforcement and judicial cooperation in criminal matters. In this field three main issues have emerged:

### 4.4.1 European Arrest Warrant (EAW) Framework Decision[40]

When the whereabouts of a person wanted for extradition are known, the European Arrest Warrant (EAW) Framework Decision permits direct transmission of the warrant between the relevant judicial authorities. However, some judicial authorities insist on the creation of an alert in SIS II, with the verification and validation processes to be carried out by all SIRENE Bureaux; this must be viewed as unnecessary and inefficient work.

The SIRENE Bureaux are also involved in the surrender or extradition procedure. Throughout the procedure, close cooperation between the judicial authorities and the SIRENE Bureau is needed to align the legal and the operational aspects of the issue and execution of the EAW. The mandatory and optional grounds for the non-recognition of an EAW and the flagging procedure concerning the alerts should also be further harmonised[41].

In conclusion, together with other matters related to the EAW, the Commission will raise with the Member States:

---

[37] Annex 1 Number 108 Commission Staff Working Document.

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

[39] Section 6.3 Commission Staff Working Document.

[40] Council Framework Decision of 13 June 2002 (2002/584/JHA) on the European arrest warrant and the surrender procedures between Member States OJ L 190, 18.7.2002, p. 1-20.

[41] Section 9.1 Commission Staff Working Document.

- the problem of creating SIS II alerts when the whereabouts of the subject of the alert are already known and confirmed; and
- the problems related to transfers, seeking to find – with the judicial and law enforcement authorities – areas where common practice can be established and procedures harmonised.

### 4.4.2 Return Directive[42]

The evaluation indicated that there are links but also inconsistencies between the provisions on entry bans as set out in the Return Directive and alerts for refusal of entry or stay as set out in Regulation (EC) No 1987/2006, even concerning the expiry date of entry bans in SIS II. This not only leads to limitations to the desired EU-wide effect of entry bans, but also to a lack of harmonisation in the criteria for issuing alerts. More harmonisation could be achieved by making it mandatory to enter all entry bans in SIS from the moment they are enforceable, but the effectiveness of the envisaged changes in SIS II could be increased by a minimum level of harmonisation across Member States when dealing with persons who are subject of a return decision or entry ban issued by another Member State[43].

In conclusion, the Commission will put forward a range of proposals on exchange of information and harmonisation of processes.

### 4.4.3 Schengen Borders Code

SIS II provides significant added value if it is checked more intensively. Member States should be encouraged to fully apply the provisions of the Schengen Borders Code which provide the obligation to directly consult SIS II as part of the border checks on third-country nationals. Member States should systematically query SIS II, i.e. carry out a 100 % check.

This conclusion is also reflected in section 4.3.4.

## 4.5 HAS SIS II BEEN RELEVANT IN VIEW OF ITS OBJECTIVES?

SIS II is today the most important and widely used information-sharing instrument in Europe, as underlined by the European Agenda on Security[44]. Only in 2015 Member States exchanged 1.8 million forms in the SIRENE Bureaux including SIS II related information[45] which clearly demonstrates the huge volume of information exchange carried out based upon SIS II alerts which makes SIS II the most relevant security platform in Europe.

The European Council and the Justice and Home Affairs Council have repeatedly pointed to the high relevance of SIS II for exchanging data on and tracking down terrorist suspects and foreign terrorist fighters and stated that all possibilities of SIS in the fight against terrorism should be exploited.

Indeed, in June 2014, the Council called upon Member States to make full use of SIS II for counter-terrorism purposes. On 30 January 2015, following the terrorist attack against the French newspaper Charlie Hebdo in Paris, the Justice and Home Affairs Ministers also stated

[42] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals OJ L 348, 24.12.2008, p. 98-107.
[43] Section 8 Commission Staff Working Document.
[44] COM(2015) 185.
[45] Section 16.4 Commission Staff Working Document.

that the potential of SIS II should be better used[46]. In its Conclusions of 20 November 2015, following the terrorist attacks in Paris, the Council drew attention to the importance of the systematic consultation of SIS II when carrying out security checks on third-country nationals illegally entering the Schengen area and when performing border checks on EU nationals. The role of SIS II as a source for intelligence and investigation by Europol was emphasised.

The Council also highlighted SIS II several times as an instrument to enhance European return policy. The European Council considered[47] that the scope of SIS II should be developed to also include return decisions[48]. On 14 September 2015 the Council adopted conclusions on more efficient use of SIS II for refusing entry and stay to irregular migrants. On 8 October 2015, the Council stated that it looked forward to proposals by the Commission, based on a feasibility study, on making it obligatory to enter all entry bans and return decisions in SIS II, notably to enable their mutual recognition and enforcement, as soon as possible. Furthermore the European Parliament also considered SIS II as a key instrument in the exchange of information on terrorist radicalisation and preventing departure as well as anticipating return in its Resolution on prevention of radicalisation and recruitment of European citizens by terrorist organisations[49].

In conclusion, in light of the security and migration issues faced and the consequent increased and broader usage of SIS II with significant results, the view of the Commission is that the underlying rationale of SIS II continues to be valid. As highlighted in section 4.3.1, to achieve this SIS must remain a flexible system, capable of swiftly addressing new operational phenomena.

### 4.6 HAS SIS ACHIEVED ITS OBJECTIVES IN AN EFFICIENT WAY? – THE COSTS OF NON-SCHENGEN[50]

Notwithstanding several findings which would improve efficiency in technical operations and working practices, SIS II is primarily an operational system and therefore an evaluation would largely expect findings in the fields of effectiveness, relevance, EU added-value and coherence with other EU initiatives. However, in such an environment, efficiency must also be studied at the strategic level. As the key compensatory measure for the removal of internal borders in the Schengen area, the question, '*Could we continue without SIS?*' must be addressed.

Development and operational costs incurred by the European Union and the Member States in respect of SIS II have to be calculated taking into consideration the technical architecture of the system, mainly the fact that it consists of three major components: central system, national systems and a communication infrastructure.

The total amount spent from the EU budget on building Central SIS II during the period 2002 to 2013 was €152 961 319 , although initially an even higher amount, of more than €175 352 417, had been allocated.

---

[46] Riga Joint Statement following the informal meeting of Justice and Home Affairs Ministers in Riga on 29 and 30 January.

[47] European Council Conclusions of 25 and 26 June 2015 (ST 22 2015 INIT).

[48] Council Conclusions on alerts in the SIS II for the purpose of refusing entry and stay pursuant to Article 24 of the SIS II Regulation upon a return decision (ST11648/15).

[49] Resolution of 25 November 2015 (2015/2063(P8_TA(2015)0410).

[50] Communication from the Commission to the European Parliament, the European Council and the Council Back to Schengen — A Roadmap. Brussels, 4.3.2016 COM(2016) 120 final.

In addition, Central SIS II incurs annual maintenance costs, which amounted to €7 794 732.35 in 2014 and €5 631 826.58 in 2015.

Since the Member States are responsible for setting up, operating and maintaining their national systems, they are also required to cover the one-time costs in terms of developing their N.SIS II[51] and annual maintenance costs. In accordance with the cost model developed in a study on possible improvements to the SIS II architecture, the average total cost of ownership of national second generation SIS II implementations, including one-time and ongoing costs in a representative sample of ten Member States studied, was €16.628 million per Member State[52].

The costs, however, have to be analysed taking into consideration that SIS II is the principle compensatory measure for the abolition of internal border controls within the Schengen area. Without SIS II, an area with no internal borders would be hardly feasible. The Commission stated, in its communication *'Back to Schengen — a Roadmap'*[53], that reintroducing internal border controls on a sustained basis within the EU would not only hamper the free movement of persons, but also would impose significant economic costs.

The Commission has estimated that:

- full re-establishment of border controls within the Schengen area would generate immediate direct costs of between €5 billion and €18 billion annually.
- Member States such as Poland, the Netherlands or Germany would face more than €500 million in additional costs for the road transport of traded goods, whilst others, such as Spain or the Czech Republic, would see their businesses paying more than €200 million in additional costs.
- border controls would cost between €1.3 and €5.2 billion in terms of time lost for cross-border workers (1.7 million workers in the EU) and other commuters.
- at least 13 million tourist nights could be lost, with a total impact of €1.2 billion for the tourism sector.
- between €0.6 billion and €5.8 billion in administrative costs would have to be paid by governments due to the need for increased staffing at border controls.

In the medium term, reintroducing border controls within the EU would entail indirect costs which may be considerably higher, given the unprecedented impact on intra-community trade, investment and mobility.

In conclusion, the costs incurred in developing and maintaining SIS II, and therefore having a well-functioning area without internal border controls, are far outweighed by the costs that would be incurred if SIS II were not in place and border controls were to be re-introduced.

## 5. CONCLUSION AND NEXT STEPS

SIS II operates against a background of the most serious concerns on security, cross-border crime and irregular migration – some of the greatest global challenges. The overall evaluation confirms the outstanding operational and technical success of the system. It is clear that no operational system, nor its legal base, will be perfect and in this spirit of continuous

[51] N.SIS II is the technical and legal term for the national SIS technical implementation.
[52] Study carried out for the European Commission: ICT Impact Assessment of Possible Improvements to the SIS II Architecture.
[53] COM(2016) 120 final.

improvement the Commission, together with the observations and support of the Member States and eu-LISA, has identified opportunities for further enhancing the effectiveness, efficiency, relevance, coherence and EU added-value of SIS II, both at central level and in some Member States where technical and operational implementation could be improved. These include the further development of the legal framework to reflect better the operational challenges in the field of security, a stronger harmonisation of the rules in the use of the system to address irregular migration as well as the better monitoring of the compliance with the data protection via statistical reporting.

SIS II achieves effective operational outcomes that can only be gained through European cooperation at both strategic and operational levels. Using all the tools available from the Treaties and the relevant legal instruments, the Commission takes a twin-track approach towards Member States: it strongly supports Member States' capacity to optimise the use of SIS II. The motivation and practical cooperation displayed between all stakeholders has led to increased and more harmonised use of the system. In cases of serious deficiencies in the implementation of SIS II the Commission is also pursuing breaches of EU law, via the 'EU-Pilot' procedure with the further option of infringement.

There are other ways in which the Commission works together with the Member States on the correct use of SIS:

- The Schengen evaluation mechanism is a major opportunity to verify the functioning and the actual use of the system on-site, which also helps to improve the situation in the evaluated Member States. An on-site evaluation re-visit is a tool available where serious deficiencies have been identified in the evaluated Member State.
- Regular meetings of the SISVIS Committee (seven times per year). The delegations include one technical and one operational expert per Member State. This Committee assists the Commission in implementing the SIS legal instruments and provides the best opportunity to address all issues of concern. The meetings provide transparency and a certain pressure on Member States to remedy any deficiencies.
- Active involvement of the Commission in every training course and conference organised on SIS II (a minimum of five times per year).
- The adoption of the Commission Recommendation on the 'Catalogue of Recommendations and Best Practices on the use of SIS II[54] on 16 December 2015, which contributes to the harmonisation of procedures and is used as a major reference document by all stakeholders.

In addition, in order to address those issues highlighted by the evaluation which require legislative change, the Commission, using its right of initiative in accordance with the Treaty on the Functioning of the European Union, intends to present a proposal to amend the legal basis for SIS by the end of December 2016. The Commission will also take into account the outcome of the deliberations of the High Level Expert Group established by the *Commission Communication on Stronger and Smarter Information Systems for Borders and Security*[55] which may result in a second proposal in June 2017.

[54] Commission recommendation establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS II [C(2015)9169/1].

[55] COM(2016) 205 final.