EN 2019

NO 20

Special Report

# EU information systems supporting border control - a strong tool, but more focus needed on timely and complete data


EUROPEAN
COURT
OF AUDITORS

# Contents

# Executive summary

I The creation of the Schengen area abolished border checks between participating countries comprising 22 EU Member States and four other European countries. However, abolishing internal borders reinforces the importance of effective control and surveillance of the Schengen area's external borders. Control of the external borders is of high interest to EU citizens and other stakeholders.

II To help border guards control the Schengen area's external borders, the EU has set up the following information systems or common frameworks for exchange of information: the Schengen Information System (SIS II); the Visa Information System (VIS); Eurodac (European Asylum Dactyloscopy Database - Fingerprint comparison system). In addition, the European Border Surveillance System (Eurosur) and the Passenger Name Record systems (PNR) provide further support to border authorities.

III Setting-up and maintaining these systems required substantial investment from both the EU and the participating Schengen states. Based on available information, we estimate that the EU budget provided over €600 million to set up these systems. Considering the increasing pressure at the EU external borders caused by recent security and migratory situations, our audit aimed at identifying aspects in the design and use of these systems that can help border guards do their job more efficiently. Furthermore, our observations and recommendations can help target the EU funding that will be made available in the next multi annual financial framework in support of these systems.

IV Our main audit question was "**Are the main EU information systems for internal security supporting border controls efficiently?**" We conclude that border guards are increasingly using and relying on these systems when performing border checks. However, some data is currently not included in the systems, while other data is either not complete or not entered in a timely manner. This reduces the efficiency of some border checks.

V We found that the systems are generally well designed to facilitate border checks and that the Member States (Finland, France, Italy, Luxembourg and Poland) we visited generally complied with the applicable legal framework. Nevertheless, some countries' national SIS II and VIS components facilitate more efficient border checks than others.

**VI** There were long delays in the implementation of IT solutions for Eurosur and PNR, both at EU and national level. This prevented border guards and other authorities of the intended benefits of these systems.

**VII** The Schengen evaluation mechanism plays an important role in securing EU external borders. Evaluations are generally thorough and methodical, and address key aspects of the systems. However, it takes a long time for the Member States to remedy weaknesses identified. This is due to a lack of binding deadlines for the adoption of evaluation reports and the implementation of corrective actions.

**VIII** Although the Member States are making increasing use of the information systems, this use could be more systematic. We carried out a survey of border guards and found that more than half of them had at some point allowed people to cross borders without consulting the systems. Furthermore, we noted a discrepancy between the number of visas issued and the number of visas checked.

**IX** Border guards use the data in the systems as their basis for making decisions that affect the safety of European citizens. The quality of this data is therefore of the utmost importance. In accordance with EU legislation, the responsibility for data quality is with the Member States. We found little reference to data quality control in the legal acts governing the European information systems. Although eu-LISA performs automated monthly quality checks of the data in SIS II, the results are available only to the Member States concerned and therefore, it is not possible for the agency or the Commission, to evaluate the progress individual countries have made in addressing data quality issues. Neither eu-LISA nor the Commission have any enforcement powers to ensure that Member States correct data quality issues in a timely manner.

**X** Border guards do not always get timely and complete data from the information systems. For example, when border guards check a name in SIS II, they may receive hundreds of results (mostly false positives), which they are legally required to check manually. This not only makes border checks less efficient, but also increases the risk of overlooking real hits. Incomplete records in SIS II also affect other systems linked to it.

**XI** Except in the case of Eurodac, there are generally no compulsory deadlines on entering data. For example, Eurosur is meant to provide real-time information on the situation at the borders. However, while some of the countries covered by our audit do indeed enter information in Eurosur on a real-time basis, others do so only once a week. Since Eurodac started operating in 2003, there has not been a single year in

which all Member States have transmitted the required information on time. Delayed transmission can lead to the wrong country being designated responsible for processing the asylum application.

**XII** We make the following recommendations to the Commission:

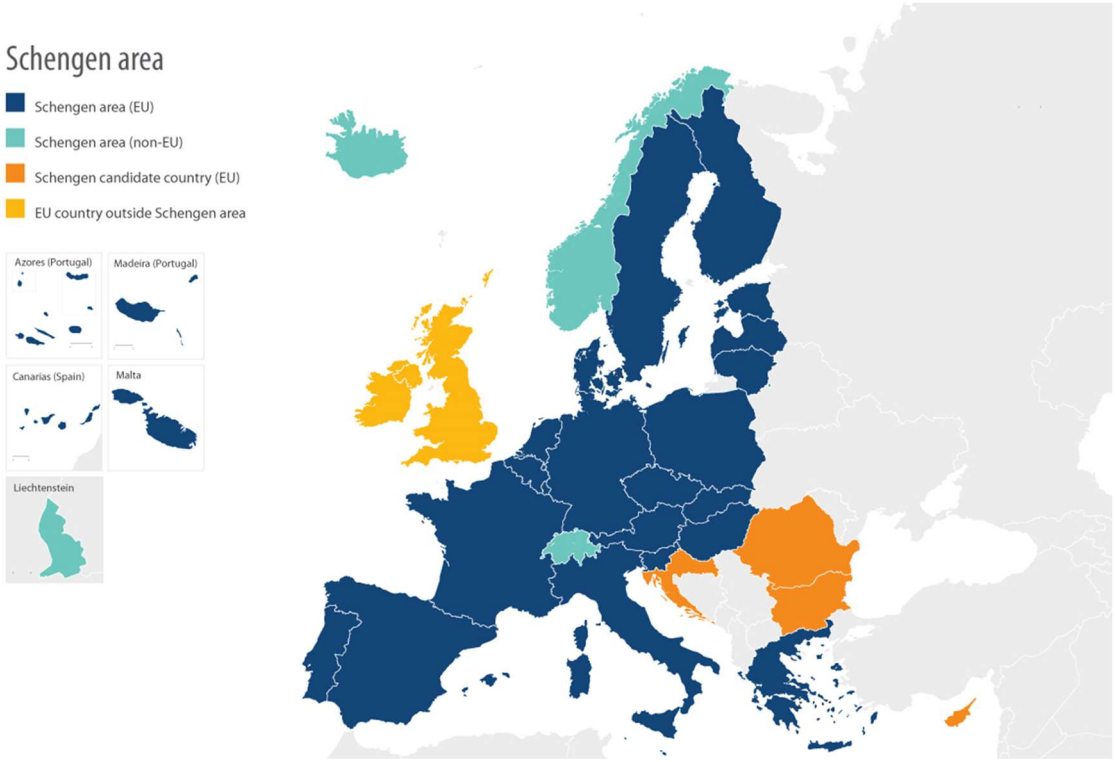
- Promote the use of SIS II and VIS training environments
- Speed up the correction of weaknesses detected during Schengen evaluations
- Analyse discrepancies in visa checks
- Improve data quality control procedures
- Reduce delays in data entry

# Introduction

## The Schengen area

**01** The creation of the Schengen area, currently encompassing 26 Schengen States, (see ***Figure 1***), enabled all travellers to cross internal borders without being subject to border checks. In addition to abolishing border checks, the participating countries agreed to a common visa policy and formalised police and judicial cooperation.

### Figure 1 – Current map of the Schengen area




*Source:* European Parliament.

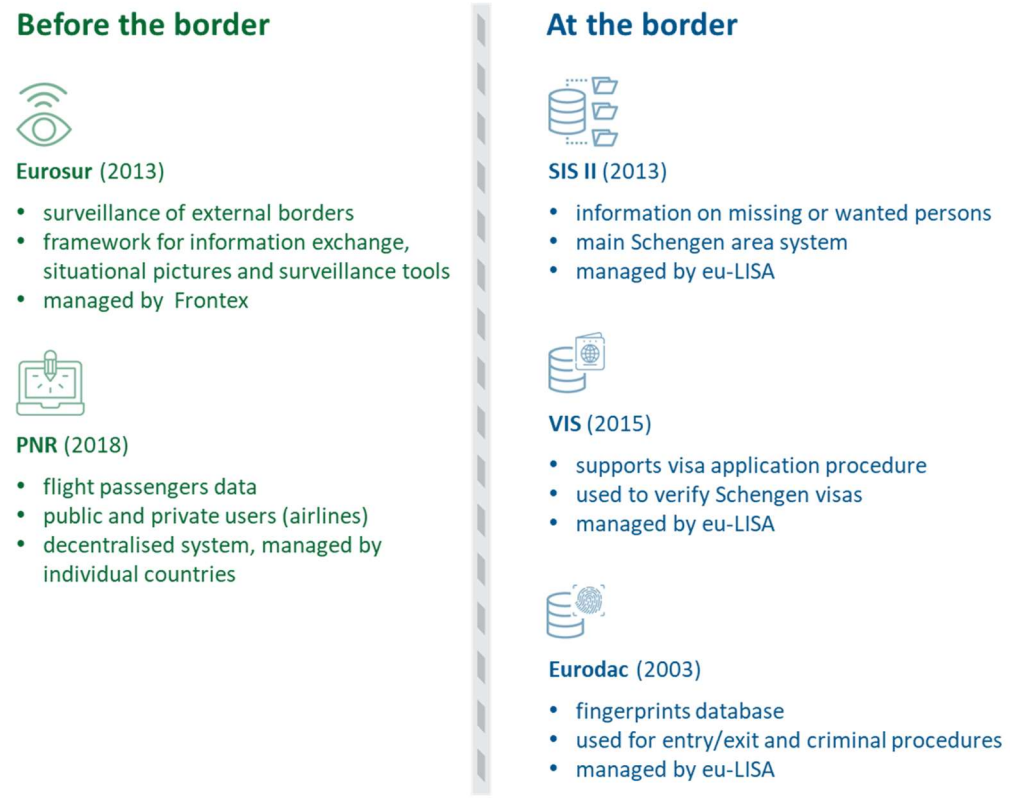
**02** Two thirds of EU citizens see the Schengen area as one of the EU's main achievements. However, nearly 70 % expect the EU to do more to protect its external borders[1].

[1] Eurobarometer 89.2, 2018.

## The information systems used to control the Schengen area external borders

**03** Abolishing internal borders requires effective control and surveillance of external borders in order to prevent crime and terrorism and to control migration. To help border guards control the Schengen area external borders, the EU set up a number of information systems or common frameworks for exchange of information. The systems most commonly used are: the Schengen Information System (SIS II); the Visa Information System (VIS); Eurodac (European Asylum Dactyloscopy Database - Fingerprint comparison system); the European Border Surveillance System (Eurosur) and the Passenger Name Record systems (PNR) (see ***Figure 2***). In addition, the EU is developing two additional information systems relevant for border security, the Entry/Exit System, the European Travel Information and Authorisation System, which should be operational in 2020 and 2021 respectively.

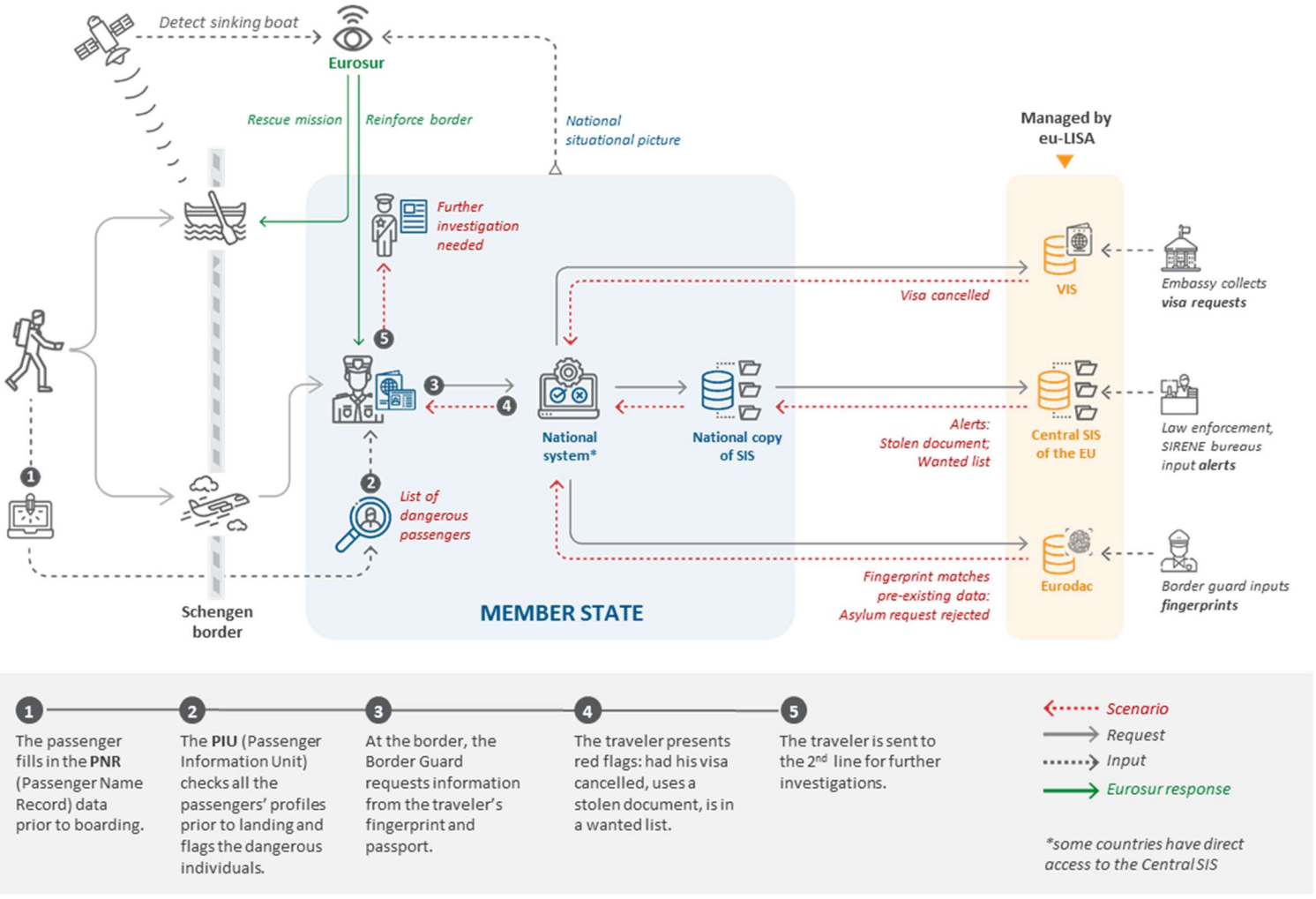
### Figure 2 – Information systems before and at the external border




*Source:* European Court of Auditors.

**04** Border guards in the Schengen States use SIS II, VIS and Eurodac to check individuals at border checkpoints. Eurosur and PNR are used to obtain information about events occurring at and beyond the EU's external borders and about passengers on flights arriving at the borders. They help to anticipate events relevant to border security. ***Figure 3*** shows how border guards are meant to use these systems during border checks, with a more detailed description, including which of the information systems are available to which countries, provided in the ***Annex***.

## Figure 3 – Use of the selected information systems for border security




*Source:* European Court of Auditors.

**05** Different national law enforcement agencies, as well as customs, visa and judicial authorities are also users of the system. At the same time, they are responsible for entering the relevant data in these systems. In the case of PNR, the information is provided by airlines.

**06** The border guards (and other authorities) using the systems in the Member States have access to the EU central systems via their own national systems, which are specifically developed for this purpose. EU lawmakers have set minimum requirements for the implementation of these national information systems in EU law[2].

**07** At EU level, the European Commission, specifically the Directorate General for Migration and Home Affairs (DG HOME), has overall responsibility for the development and funding of the information systems, except PNR which does not have an EU-level central component (but can benefit from EU funding). Since 2012, the Commission has tasked the European Union Agency for the Operational Management of Large-Scale Information systems in the Area of Freedom, Security and Justice ("eu-LISA") with storing data and maintaining SIS II, Eurodac, and VIS. Eurosur, meanwhile, is managed by the European Border and Coast Guard Agency (EBCGA), known as Frontex, and the Member States.

---

[2] Regulation (EU) No 1987/2006 for SIS II, Council Decision 2007/533/JHA on SIS II No 767/2008 for VIS, Regulation (EU) No 603/2013 for Eurodac and Regulation (EU) No 1052/2013 for Eurosur. Directive (EU) 2016/681for PNR.

**08** Based on available information, we estimate that the EU budget provided over €600 million[3] to cover the cost of setting up the EU level components for the systems covered by our audit. The total annual cost of operating the systems was approximately €61.5 million[4]. In addition, Member States contribute towards the cost of developing and maintaining the national systems from their own budgets. Although information on Member States' spending on their national systems is not always available, there are indications that these amounts are significant. For example, Member States spent approximately €235 million on setting up SIS II in addition to €95 million paid for from the EU budget[5].

[3] The amount is based on information included in documents published by the Commission or information obtained from their accounting system (for SIS II and VIS). This amount does not include the cost of developing Eurodac, for which no aggregated figures were available.

[4] This includes eu-LISA's 2017 commitments directly related to the information systems covered by the audit and Frontex's 2017 commitments related to Eurosur, and SIS/VIS/Eurodac implementation of payments appropriations from DG Home 2017.

[5] European Court of Auditors, Special Report 03/2014, "Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)".

# Audit scope and approach

**09** The EU is continuously working to improve the security of EU borders, which is an important topic for EU citizens. Considering the increasing pressure at the EU external borders caused by recent security and migratory situations, our audit aimed at identifying aspects in the design and use of these systems that can help border guards do their job more efficiently. Furthermore, our observations and recommendations can help target the EU funding that will be made available in the next multi annual financial framework in support of these systems.

**10** The main audit question was:

- Are the main EU information systems for internal security supporting border control efficiently?

**11** This audit question was broken down into the following sub-questions:

- Are the EU information systems for internal security well designed to facilitate efficient border checks?
- Are the EU information systems for internal security providing border guards with relevant, timely and complete information during border checks?

**12** Our audit covered the following five systems: the Schengen Information System (SIS II); the Visa Information System (VIS); Eurodac (European Asylum Dactyloscopy Database - fingerprint comparison system); the European Border Surveillance System (Eurosur) and the Passenger Name Record systems (PNR).

**13** We assessed how well the systems (both national and central components of the EU systems) allowed the border guards and other officials to check individuals entering the Schengen area at authorised border crossing points[6].These include land border crossing points, sea ports and airports (which, for some Member States, are the only external EU borders).

---

[6] We have already covered some issues linked to illegal migration in special report 06/2017 "EU response to the refugee crisis: the 'hotspot' approach" and will further analyse these issues in forthcoming publications.

**14** We reviewed and analysed the strategic documents, evaluations and statistics relating to the five systems covered by our audit, as well as a variety of documents relating to their implementation at both national and EU level. In addition, we visited border checkpoints and interviewed border authorities in Finland, France, Italy, Luxembourg and Poland. We also interviewed staff of DG HOME, Frontex and eu-LISA.

**15** We also conducted a survey of EU border guards in 28 EU Member States and 4 Schengen associated states (Iceland, Liechtenstein, Norway and Switzerland) to obtain their views as users of the systems. We received 951 replies.

# Observations

## The information systems' design facilitates efficient border checks, but resolving weaknesses takes a long time

**16** We assessed whether the Schengen States we visited had set up the information systems as and when required by the relevant EU legislation. We also examined the Schengen evaluation mechanism and the extent to which the Schengen States had used the available EU funding to set up and improve their national systems.

### Information systems were generally in line with EU requirements but did not operate with equal efficiency

**17** While each Schengen State is solely responsible for protecting its own borders, effective cooperation between them to protect the area requires a certain level of harmonisation of border checks. Minimum governance requirements help ensure the consistency and quality of border checks and of the data entered in the information systems.

**18** Each Schengen State must set up its own complementary national systems, which connect to the central EU systems. The Schengen States we visited had all done so in line with the requirements defined in the relevant legislation. Nevertheless, we found that, while all the systems met the common minimum requirements, not all national systems were equally efficient. The following paragraphs provide some examples of this.

**19** Some countries do not make all the functions offered in the central EU systems available through their national systems, thus reducing the efficiency of border checks. For example, the central SIS II system offers the option to store and check fingerprints. This is important because it is not always possible to uniquely identify a person from basic personal data such as a name or a date of birth. Such data can be forged, or a person can refuse to provide it. Fingerprints make it possible to identify a person with a much higher degree of certainty. However, the option perform biometric searches on the basis of fingerprints stored in SIS is not yet available in all Schengen States' national systems, as some require more time than others to implement the necessary technical solutions. When fingerprint identification was available at the central level, only 10 Schengen States confirmed that they were ready to use it.

**20** Border guards checking a visa or passport sometimes receive error messages from the systems. These can have several causes, such as fingerprints of insufficient quality, connectivity issues or problems reading the visa. While the central EU systems usually indicate the nature of the error, some national systems, such as Luxembourg's and Finland's, merely signal that an error has occurred without providing a diagnosis. This means the border guards have to investigate the cause of the error and potentially refer the passenger for further verification (known as the "second line of control"), thereby delaying their checks and the passenger's journey.

**21** In the case of SIS II, Schengen States can either access and submit queries to the central database or create their own national copies for this purpose. While most of them operate their own national copies, some (Denmark, Finland, Liechtenstein, Norway and Slovenia) connect directly to the European database. Where Schengen States use national copies of SIS II, these must be synchronised with the central European database at all times in order to ensure that border checks are based on the most up-to-date information. However, in two of the countries in our sample (Poland and France), evaluations have indicated discrepancies between records in the national copies and in the central database.

**22** We also found that certain legal constraints at the Member State level (rules on data protection and national security) prevented the efficient sharing of human resources. In fact, border guards visiting another Schengen country (e.g. to assist in reinforced controls during the migration crisis in Greece and Italy) are not allowed to use that country's national systems. As a matter of principle, they cannot conduct controls independently, but only assist the national border guards. While they may provide varying degrees of help on the second line of control (e.g. a Schengen State might use an expert on forged documents from another Schengen State), they can provide only limited help during the document checks at border checkpoints (at the first line of control). Another barrier is the linguistic challenges linked to working in another Schengen State.

**23** The benefit border guards derive from the systems depends on how well trained they are to use them. We found that there was no training environment for SIS II and VIS implemented at national level in the Member States we visited, so border guards had to practise on these "live" rather than in a "safe" environment where they could experience features and scenarios that they do not encounter frequently on the job (e.g. a hit identifying a suspected terrorist at a border checkpoint, or a missing minor).

## Delays in the implementation of Eurosur and PNR prevented border authorities from sharing important information

**24** For Eurosur and PNR, the implementation arrangements were different to those systems developed and managed by eu-LISA. For differing reasons, the implementation of both systems suffered from some missed deadlines and delays. As a result, important information that these systems were intended to provide remained unavailable for several months.

**25** Eurosur was developed by Frontex (the European component) and by the Member States (the national components). Its end-user interface is the same for all participating national authorities. The system is intended to enhance cooperation between Frontex and the EU Member States to improve their awareness of and responsiveness to the situation at the EU's external borders. Member States should contribute with information about the situation at their borders (known as their "national situational pictures", showing information on unauthorised border crossings, cross-border crime, crisis situations and other events relevant to the control of the external borders) in order to build up shared intelligence and a picture of the Europe-wide situation. This is useful, for example, for prioritising the deployment of border guards or detecting suspicious vehicles/vessels.

**26** The delays in relation to Eurosur concerned the creation of National Coordination Centres (NCCs). NCCs coordinate information exchange between all the authorities responsible for external border surveillance. The Eurosur regulation required Member States to establish their NCCs by December 2014. However, an evaluation nearly four years later found that several Member States were still not fully compliant with the requirements[7]. In addition only half of the Member States were sharing voluntary information about their deployment of surveillance resources and additional information from their national situational pictures.

**27** The implementation of Eurosur was also behind schedule at EU level. Frontex did not obtain the required security certification for its network until the end of 2017 – three years after the entry into force of the legislation. Without this certification, it was not possible to share classified information over the Eurosur network. The delays in the implementation of Eurosur meant that the EU-wide situational picture was incomplete, which hindered cooperation between the Member States.

---

[7] Report from the Commission to the European Parliament and the Council on the evaluation of the European Border Surveillance System (EUROSUR), COM(2018) 632 final.

**28** PNR is not yet fully operational. Unlike the other systems, it was set up by means of a directive rather than a regulation. Consequently, it was left up to the Member States to set up their own PNR systems separately, without any common European platform. The decision in favour of decentralised implementation was mainly driven by a lack of consensus on the protection, storage and disclosure of personal data.

**29** Many Member States did not implement PNR in a timely manner. Fourteen Member States failed to implement the rules on Passenger Name Record data on time[8]. They were supposed to comply with the directive[9] by 25 May 2018. However, by the end of March 2019, 10 months after the deadline, Spain, the Netherlands and Finland still had not notified the Commission of any measures taken nationally to implement PNR[10].

**30** PNR requires passenger data to be transmitted from all flights into and out of the Schengen area. At the time of our audit, none of the Member States visited, except Luxembourg, had concluded agreements for this purpose with all relevant airlines.

**31** PNR was designed as an important tool to prevent, detect and investigate terrorism and other forms of serious crime. Comparing PNR data with information contained in security databases allows the relevant authorities to detect dangerous individuals. The fact that some PNR systems are not yet in place deprives border authorities in those countries of advance information about high-risk individuals crossing their borders.

**32** Since PNR only collects passengers' identification and travel data, it needs other databases to verify whether a given passenger poses a security threat. Most Member States use SIS II for this purpose. However, the regulation allows for different interpretations. For example, France has interpreted the SIS II regulation in a way that does not allow it to use SIS II queries on passenger lists. In practice, this means that when checking passenger lists for suspected terrorists, France only uses information from its national databases. If there is an alert on a suspect in SIS II, and that suspect is

---

8 http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm

9 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

10 http://europa.eu/rapid/press-release_MEMO-19-1472_en.htm

known to other European authorities but not to the French authorities, their PNR check will not detect that person.

## Schengen evaluations assess national border checks, but resolving weaknesses takes a long time

**33** Since 2013, the Schengen States and the Commission have been jointly responsible for implementing the monitoring and evaluation mechanism provided for in the rules on the Schengen area (the "Schengen Acquis"). The aim of the mechanism is to ensure that the Schengen States apply the Schengen rules effectively, consistently and transparently. We examined whether the aim of the mechanism is being achieved.

**34** The current multiannual evaluation programme was established in 2014 for the 2015-2019 period and covers all 26 Schengen countries. Each country is evaluated once during the five-year period

**35** ***Box 1*** describes a standard evaluation visit. Evaluation team members are designated by the Schengen States based on a call for designations by the Commission (each evaluation has a separate call for designations, with a two weeks deadline for Schengen States to designate the reviewers). Reviewers from eu-LISA can participate in these visits, but they do not take part in them regularly. The cost of Schengen evaluations is relatively low compared to the expenditure on the information systems. For the 2014-2018 period, the Commission allocated €11.9 million to Schengen evaluations. The current multiannual programme has been implemented as planned through annual evaluation programmes.

**Box 1**

**Schengen evaluation team's visits to Schengen States**

In July the year before they are due to receive an evaluation visit, the Member States concerned receive a standard questionnaire, to which they have eight weeks to reply. The evaluation team prepares its visits based on the replies received.

Evaluation visits usually last one week. Teams consist of maximum eight experts appointed by Schengen States, plus two representatives from the Commission. The team members have different types of expertise, allowing them to cover all aspects of the Schengen Acquis. Each team is headed by two lead experts (one from the Member States and one from the Commission), responsible for the content and quality of the final report.

The visits start at a strategic level, with meetings at ministries and border authority headquarters, followed by activities at an operational level. The evaluation team members are allocated to their different areas of expertise and meet with different national practitioners, such as border guards, police officers and IT experts.

For example, during the 2017 Schengen evaluation of the implementation of SIS II in France, the team visited 38 on-site locations, including the National SIS II IT centre, police stations, customs offices, ports, airports and train stations.

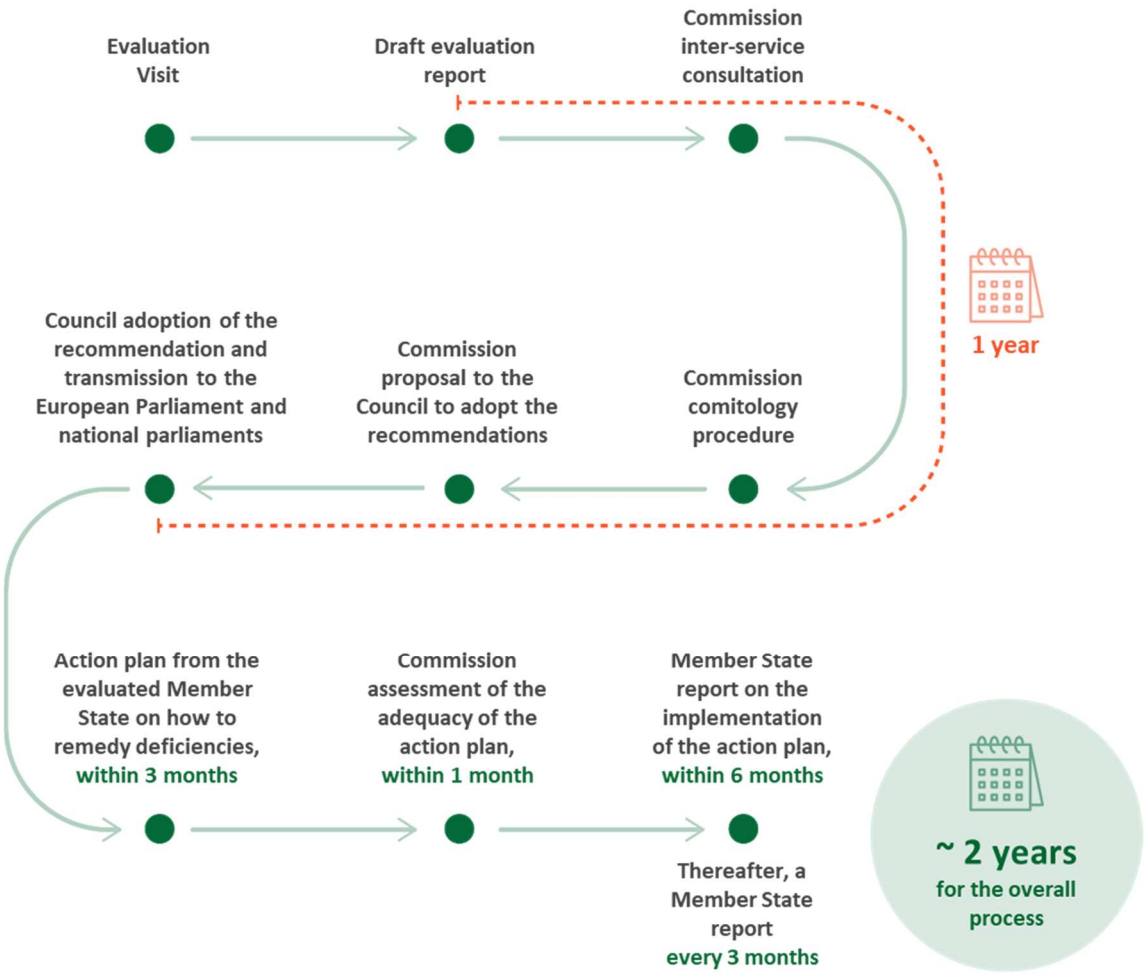
**36** We examined the Schengen evaluations of the countries we visited. We found that these were thorough and methodical, and addressed key aspects of the systems. They provided a detailed set of operational recommendations and specific recommendations on improving the information systems. However, it can take several years to address identified weaknesses.

**37** The draft evaluation report is completed six weeks after the evaluation mission, but it can take the Commission one year to adopt the report, and the Council to adopt the recommendations. This involves numerous procedures for consultations with the Schengen State and the Commission. There are no agreed deadlines for these consultations.

**38** Once the Council adopts the recommendations, the Schengen States concerned have three months to present an action plan to address the Council's recommendations. This action plan needs to be reviewed and approved by the Commission and the evaluation team.

**39** There is no deadline for the implementation of the action plans, although the Schengen States must start to report on their implementation six months after the plan is approved. This means that from the time a shortcoming is detected, it could take almost two years before a Schengen State starts to report on the corrective action it has taken. ***Figure 4*** shows the procedure following an evaluation visit.

## Figure 4 – Schengen evaluation mechanism procedural steps




*Source:* European Court of Auditors.

**40** So far no Schengen State has yet been subject to more than one announced evaluation visit under the current cycle of evaluations. The Commission relies on Schengen States' own reporting on their implementation of the agreed action plan. There is therefore a risk of deficiencies remaining unaddressed until the next round of evaluations five years later. It could then take a further two years for that country's authorities to implement corrective action.

**41** The Commission can suggest follow-up visits if a Schengen State fails to implement its action plan, but there are no other mechanisms in place to enforce

implementation. In theory, if persistent serious deficiencies are identified in a Schengen State in the field of management of the external border, the Council may, based on a proposal from the Commission, recommend that the country reintroduce controls at its borders with other Schengen States.

**42** Under the regulation from 2013 on the Schengen evaluation mechanism[11], the Commission is required to report annually to the Parliament and the Council on the evaluations carried out, the recommendations made and the state of play with regard to remedial action. The Commission has not yet produced such a report.

**43** With the exception of Finland, whose evaluation report had not been completed at the time of the audit, all the Schengen States we visited had been subject to evaluation. We followed up on their progress in implementing their action plans and found a variety of implementation rates. According to the evidence provided, Poland had implemented 79 % of its recommendations two years after the evaluation visit, France had implemented 87 % of the recommendations four years after the evaluation visit and Luxembourg, which was evaluated in 2018, has implemented 92 % of the recommendations. The evidence from Italy suggested that, two years after the evaluation visit, the country was in the process of implementing 15 % of its recommendations.

## EU Member States make only limited use of available EU funding to improve information systems for border control

**44** The main EU instrument to support border control is the Internal Security Fund (ISF) with an initial allocation of €3.8 billion for the 2014-2020 period. It consists of:

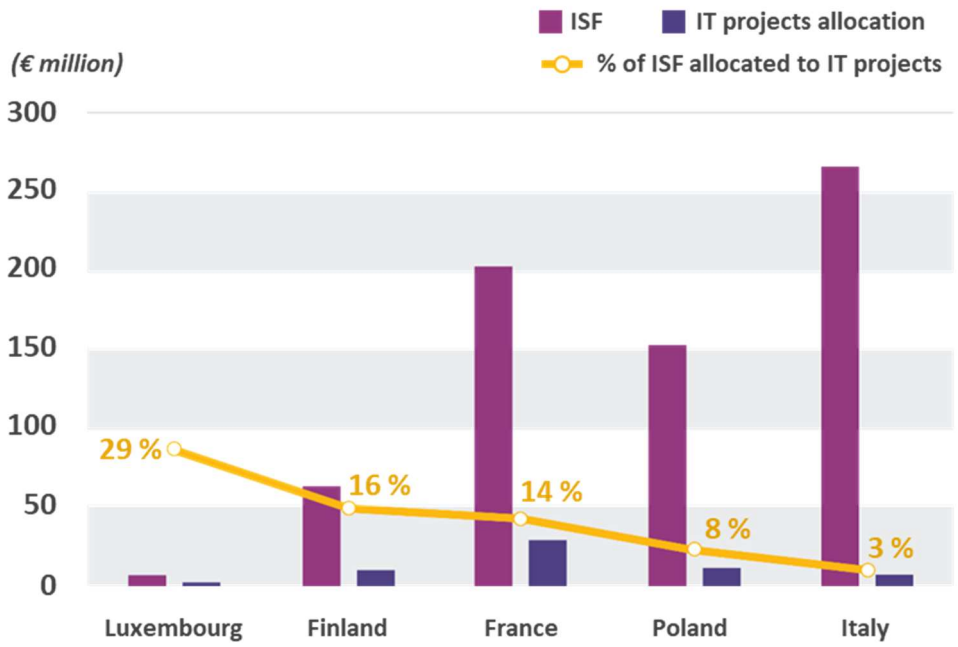
- ISF Borders (€2.76 billion), providing support for the management of external borders and the common visa policy. All EU States except Ireland and the United Kingdom participate in the implementation of the ISF Borders instrument. The four Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland) also participate in the ISF Borders and Visa instrument.
- ISF Police (€1.04 billion), providing financial support for police cooperation, preventing and combating crime, including migrant smuggling. All EU States except Denmark and the United Kingdom participate in the implementation of the ISF Police.

[11] Article 20 of Council Regulation (EU) No 1053/2013 of 7 October 2013.

**45** Most of the Member States did not report any significant expenditure until 2017. As spending started late, the Member States have been slow to use the money. According to the Commission, the primary reason for this is the heavy procurement procedures involved. The Member States covered by the audit, also noted the additional administrative burden involved. For example, they noted that even a small increase in the amount allocated to a national programme requires a complete revision of that programme.

**46** The countries covered by our audit, dedicated between 3 % and 29 % of their Internal Security Fund allocations (€61.2 million) to the five systems audited (see ***Figure 5***). Of this, they allocated 43 % (€26.5 million) to maintenance projects and 57 % (€34.7 million) to extension projects. They have mostly used this money for maintenance of SIS II and VIS and extensions of Eurosur and PNR.

## Figure 5 – Percentage of ISF funding allocated to IT projects




*Source:* European Court of Auditors based on the European Commission data.

## Border guards do not always get complete data from the systems, which undermines the efficiency of checks

**47** We assessed the extent to which the Member States share relevant, timely and complete information through the information systems covered by the audit. We reviewed available statistics in order to assess the extent to which the Schengen countries are using the systems for their border checks and for exchanging information. In addition, we examined whether these countries entered complete data promptly.

## Member States are making increasing use of the systems to share information, but checks could be more systematic

**48** From the moment individuals present themselves at a border checkpoint to the Schengen area, border guards need European information systems to help them confirm the person's identity and verify that they are authorised to enter the Schengen area.

**SIS II**

**49** Any Schengen State with information about a person to be intercepted at the border (as prescribed by the relevant legislation) should create an alert in SIS II. This allows border guards in any participating country to act upon it when they encounter that individual during border checks (see ***Box 2***).

### Box 2

### Hitting the right target

When a person presents a travel document, the border guard uses a scanner, which reads an identifier on the travel document. The most modern documents contain an electronic chip, while older documents have a special code at the bottom of the page (known as the machine-readable zone or MRZ) and some documents have none (for example, most Italian ID cards). If the document number cannot be retrieved by the scanner, a border guard can enter it in the system manually.

Based on the data transferred to the computer, a query on a person is sent to the national or European SIS II databases. If there is a match between a record in the database and the data collected by the border guard, it is called a *hit*.

If the initial alert recorded in the database was created in a country other than the one from which the query is sent, the hit is called a *foreign hit*.

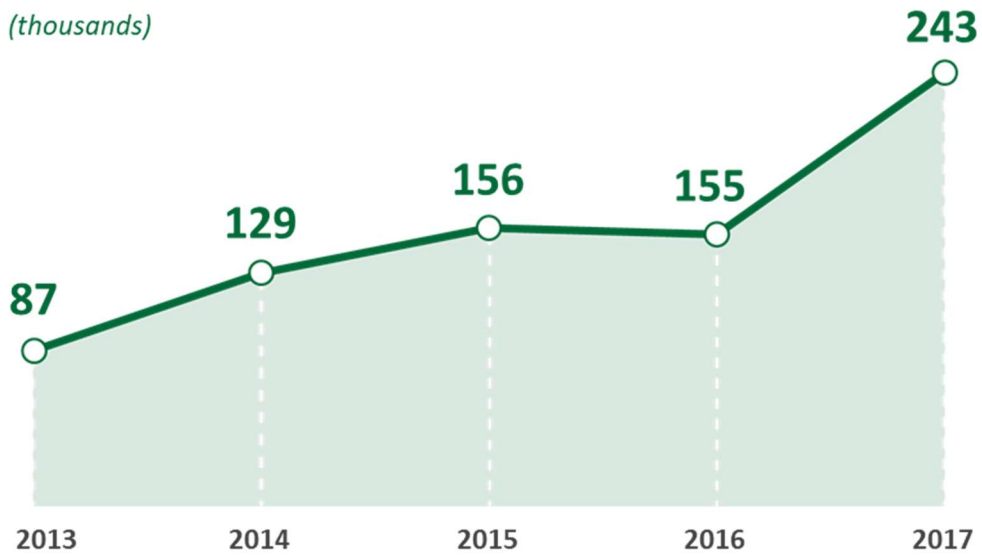
Hits may occur if the relevant authorities have registered a person as wanted, or the travel document has been flagged in the system.

However, sometimes the authorities issuing an alert do not have all the information they need to identify a person uniquely. Matches may therefore occur for someone who is not actually the wanted person but who has the same name. This type of match is called a *false positive*. In such cases, border guards must take further steps in order to establish that person's identity.

Biometrics (i.e. fingerprints) are generally regarded as a way to identify a person uniquely, which is why an increasing number of alerts in SIS II contain fingerprint information.

**50** We found that, between 2013 and 2017, the number of hits relating to wanted persons and objects based on alerts originating in other countries almost tripled (see ***Figure 6***).

## Figure 6 – Number of hits in SIS II based on alerts from other countries



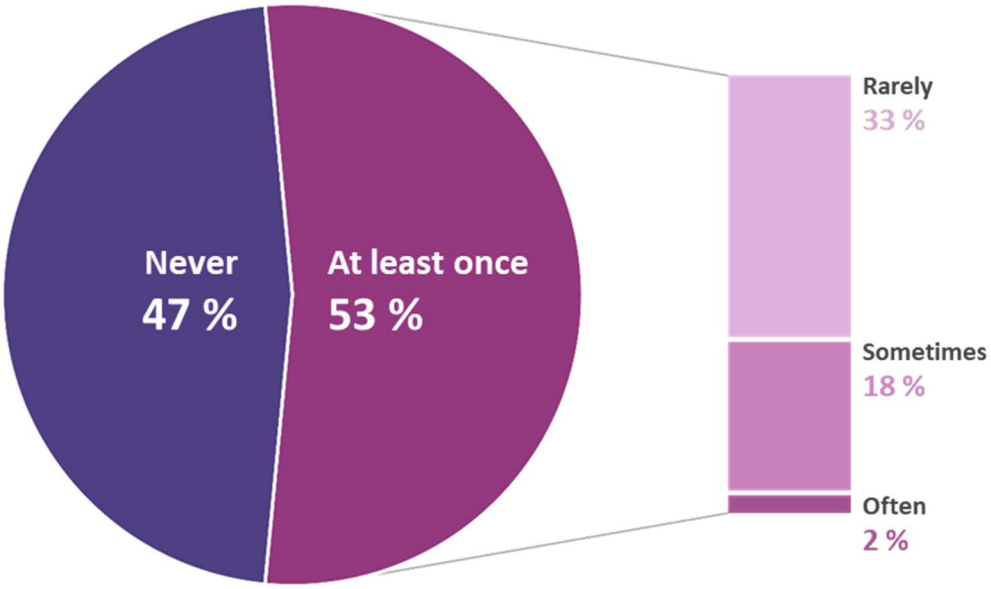

*Source:* ECA based on data from eu-LISA.

**51** The increased number of hits is consistent with the steady increase in the number of alerts in SIS II, from around 50 million in 2013 to over 76 million in 2017. Most of the alerts (76 %) concern lost or stolen documents.

**52** According to Eurostat data[12], the number of third-country nationals refused entry at the external borders ranged from a low of 440 000 in 2017 to a high of nearly 500 000 in 2009. The information systems provide the necessary support for identifying the most typical reported reasons for refusal. However, Schengen States do not always specify or record the reason why an individual was refused at the external border.

**53** As described above, the number of queries submitted to the information systems is constantly growing. National authorities stated during the audit interviews that they check every individual who tries to cross the external border. However, our survey revealed that more than half of the border guards had been in a situation where they had to decide whether to let someone through without consulting the systems.

**Figure 7 – Survey: Have you ever had to take a decision about letting someone in without being able to consult the data from the system?**




*Source:* ECA survey.

**54** The use of the information systems also depends on the external environment in which checks are carried out. Some types of border crossing are more challenging than others. For example, checks carried out on board ships often suffer from connectivity issues. During our visits to two countries, we observed such problems preventing complete border checks. Conducting checks on moving trains poses similar technical challenges.

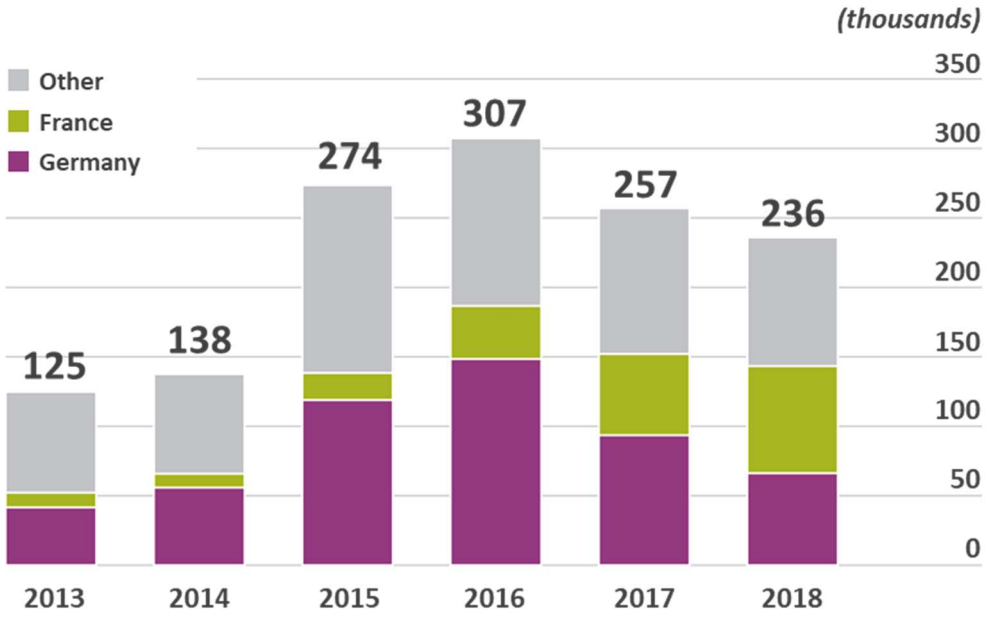
[12] https://ec.europa.eu/eurostat/web/products-datasets/-/migr_eirfs

**Eurodac**

**55** Another example of increased data exchange among Schengen States is through the Eurodac system, which allows them to register asylum seekers and persons attempting an irregular border crossing by taking their fingerprints. Since 2003, there has been an agreement[13] between EU Member States that asylum applications should be processed in the country where the applicant first declares his or her intention to seek asylum. Whenever a national administration compares a person's fingerprints against those registered in Eurodac, a hit is returned if that person has previously applied for asylum in another EU country and should be returned there.

**56** The number of applications for asylum made by individuals who had already lodged an application for asylum in another Member State grew significantly until 2016, which was the peak of the migration crisis. Most applicants tried to seek asylum in France or Germany having initially arrived in another EU country, as shown in ***Figure 8***.

## Figure 8 – Asylum seekers with a previous application in another Member State




*Source:* ECA based on data from eu-LISA.

[13] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (the "Dublin II regulation").

**Passenger Name Record**

**57** PNR is a new system. While the Member States share a common legal basis for its implementation, their ability to use the system to exchange information remains limited, as explained in paragraph ***28***.

**Eurosur**

**58** The use of Eurosur is very uneven between Member States. Between 2013 and 2017, over 140 000 incidents were recorded in Eurosur. However, numerous participating countries did not record a significant number of incidents[14]. Austria, Belgium, Cyprus, Czech Republic, Germany, Denmark, France, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Sweden and Slovenia recorded below 5 000 incidents each, while Hungary, the most active country, registered over 25 000. The type of information that Member States share also varies. They can choose whether to enter only compulsory information (e.g. data relating to illegal migration and cross-border crime and information from the surveillance of land and sea borders) or extended additional information such as information on legal or administrative measures after interception and information on air borders and checks at border checkpoints. For example Finland has chosen to share all the information from its national situational picture, both compulsory and optional, while Poland and France only enter compulsory information.

**VIS**

**59** The Schengen States have a common visa policy. They can issue common short-stay visas that allow the holder to stay for up to 90 days in any of the 26 Schengen countries. In 2018, the Schengen States issued over 14 million short-stay Schengen visas[15].

**60** The system makes it possible to verify the identity of a Schengen visa holder anywhere within the Schengen area. A Schengen visa holder may cross the area's external borders multiple times and may do so in different Schengen States. VIS statistics show the number of times visas are queried at the borders. In the first nine months of 2017, 35 million visa checks were carried out at the borders, compared to

---

[14] Evaluation of Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System, SWD(2018) 410, 19.12.2018.

[15] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy#stats

12 million visas issued in that period. The number of checks carried out varies significantly between the Schengen States.

**61** We found that between October 2015 and September 2017, the five countries (France, Germany, Italy, Spain and Greece) that issued the highest number of visas performed fewer visa checks at their borders than the number of visas issued. For a combined total of nearly 18 million visas issued these countries conducted fewer than 14 million checks.

**62** In theory, this could be because a significant number of travellers with visas issued by those countries entered the Schengen area via another country, or deferred or cancelled their journeys. However, given that most travellers are likely to apply for a visa from the country they intend to enter, and that a Schengen visa costs money[16], it could indicate that visas are not systematically checked at all border checkpoints.

## Information was not complete in some of the systems

**63** The quality of the data in the information systems is of the utmost importance. Entering data in the system is the responsibility of judicial and law enforcement authorities, as well as Member States' national border authorities. The border guards use this data as their basis for making decisions that affect the safety of European citizens.

**64** In accordance with EU legislation, the responsibility for data quality lies with the Member States. Therefore we found little reference to data quality control procedures at EU level. Only the Eurodac regulation laid the foundation for a fingerprint quality control framework by making eu-LISA responsible for setting quality standards.

**65** The SIS II regulation did not involve the Commission or eu-LISA in the data quality process. Instead, it made Member States responsible for the accuracy, timeliness and relevance of the data in the system[17]. The national offices coordinate the functioning

[16] A Schengen visa costs €60.

[17] Article 34 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006.

of SIS II and are responsible for coordinating the quality control of information entered in the systems[18].

**66** Data quality gained greater prominence in 2018 with the new eu-LISA regulation[19], which assigns the Commission and eu-LISA responsibilities in the process of assuring data quality. The regulation introduced the requirement for eu-LISA to carry out automated data quality checks and report on data quality indicators for SIS II, VIS and Eurodac.

**67** Since April 2017, eu-LISA has performed automated monthly data quality checks on certain SIS II alerts (e.g. for problems with transliteration of names from languages with non-Latin alphabets, or automated controls skipped by entering generic words such as "UNKNOWN"). These checks generate a report listing the individual alerts with potential quality issues and transmit it directly to the country concerned. However, in line with the legal requirements on data protection, eu-LISA itself cannot see these individual alerts – the agency can only see the aggregate numbers of quality issues for each type of alert and each country.

**68** The monthly reports show approximately 3 million warnings of potential data quality issues (out of an average total of 82 million records) meaning that the data might not meet the SIS II data quality requirements. We found that neither eu-LISA nor the Commission have any enforcement powers to ensure that Member States correct data quality issues in a timely manner. Indeed, the monthly reports show no significant reduction in the number of SIS II quality warnings. Furthermore, since eu-LISA cannot see the individual alerts, it has no way of knowing whether the alerts in a given month are new or remain unresolved from previous reports. Besides this overview, which is of limited use as a quality management tool, we did not obtain any evidence of other automated data quality checks at EU level.

**69** According to the Commission's evaluation of SIS II[20], Schengen States have cited data quality problems as a frequent and recurring issue. Overall, two main data quality

---

[18] Article 7, idem.

[19] Article 12 of Regulation (EU) No 2018/1726 on the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice (eu-LISA).

[20] 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, 21.12.2016, p. 11.

issues emerge from the countries we visited: one concerns the completeness of the data, and the other concerns delays in entering data in the systems.

**70** The data in the system should allow border guards to uniquely identify the person being checked and determine whether to let him or her through. We found that, sometimes, border guards do not get adequate information from the system to make this decision.

**71** For example, we found alerts where the first name of the person was inserted as a surname and missing or incomplete dates of birth making it difficult to identify the person[21]. As a result of such issues, when border guards check a name in SIS II, they may receive hundreds of results (mostly false positives), which they have to check manually. This not only makes border control less efficient, but also increases the risk of real hits being overlooked.

**72** Incomplete records in SIS II also reduce the efficiency of other systems linked to it. For example, when Schengen States' authorities are checking passenger information on the PNR list, they normally check it against alerts in SIS II. Incomplete alerts generate a large number of false positives wrongly indicating that a passenger is suspect. Since every alert must be checked manually, this generates a significant workload for the Passenger Information Units processing the PNR lists. Furthermore PNR data can also be incomplete. The data provided from their reservation systems may contain as little as the passenger names and the flight number.

**73** VIS can only record short-term Schengen visas, even though Schengen States are still using over 200 different types of national visas and residence permits to allow third-country nationals to enter and travel around the Schengen area. These permits are registered only in national databases, which are not shared with other countries. Almost 2.6 million such permits were issued in the Schengen area in 2017[22]. There is currently no legal basis for recording these permits in the central VIS system.

---

[21] Numerous Member States have cited data quality problems as a frequent and recurring issue according to the Commission in its evaluation of SIS II. 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, 21.12.2016.

[22] Eurostat statistics (first permits in 2017): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_resfirst&lang=en

**74** The Commission has identified this information gap and is currently working on a regulation to address the issue[23]. However, since these travel documents can be valid for up to 10 years, they will remain outside the system for years before the information gap is closed.

**75** In relation to Eurosur, one weakness is that Member States submit their reports in different formats. This means that the information cannot be easily aggregated and may not even be accessible to other Member States for technical reasons.

**76** Data is usually entered into Eurosur manually. When there is an increase in events at the borders, it can be difficult for an operator to record these quickly in the system. Data quality can suffer as a result[24]. Furthermore, some Member States report incidents on a case-by-case basis, while others provide only aggregated data. Some Member States create an incident report for each individual, while others create one incident report covering numerous people. This renders the statistics on the number of incidents reported by Member States irrelevant, because they do not show the true scale of the problem. It also makes it difficult for Frontex to monitor developments and prioritise the allocation of additional resources as needed.

## Events are not always recorded promptly in the systems

**77** Border guards need to have access to up to date information on people crossing the border in order to do their job effectively. Sometimes, however, Member States do not enter information as soon as they become aware of it.

**78** PNR data is generated during reservation, and airlines are subject to fines for late delivery of passenger lists. For VIS, the data is automatically generated when a visa is issued. For Eurodac there is a legal deadline for entering information on asylum

---

[23] COM(2018) 302, Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA.

[24] Source: Evaluation of Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), 12.9.2018, p. 44.

applicants. However, SIS II and Eurosur do not have such specific time limits for entering information[25].

**79** Eurosur is meant to provide real-time information on the situation at the borders, but the timeliness of the information depends on how promptly the Member States enter it. Some of the countries covered by our audit do indeed enter information into Eurosur on a real-time basis, while others do so only once a week. This means that an incident at the border (i.e. a large group of migrants arriving) might not appear in the European system until up to one week later.

**80** The Dublin regulation[26] states that the country through which the asylum seeker first entered the European Union is responsible for examining an application for asylum. Member States have a maximum time limit of 72 hours[27] to take fingerprints and transmit them to Eurodac, starting from the moment a person seeks asylum or is apprehended during an irregular border crossing. If the person seeking asylum moves to another Member State, the delayed transmission can lead to the wrong Member State being designated responsible for processing the asylum application (see paragraphs ***55***-***56***).

[25] PNR data is generated during reservation, and airlines are subject to fines for late delivery of passenger lists. For VIS, the data is automatically generated when a visa is issued.

[26] Regulation (EU) No 604/2013.

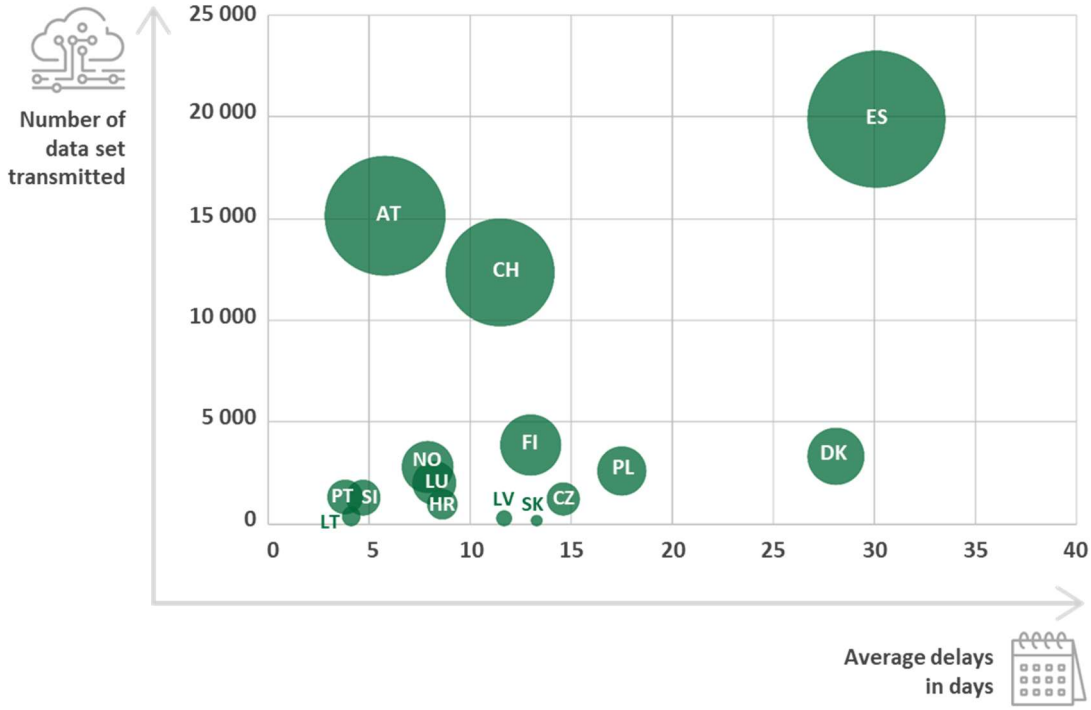
[27] Article 9(1) and Article 14(2) of the Eurodac Regulation.

## Picture 1 – Collecting fingerprints for registration in Eurodac



**81** Since Eurodac started operating, there has not been a single year in which all Member States have transmitted the required information on time. Fifteen countries' average transmission times exceeded the time limit for entering the fingerprints in 2017 – see ***Figure 9***. While the regulation foresees derogations to the data entry deadlines, there is no mechanism in place to distinguish these from irregular delays.

## Figure 9 – Average delays in transmitting fingerprints in 2017




*Source:* ECA based on data from eu-LISA, Annual report on the 2017 activities of the Eurodac central system.

**82** As ***Figure 9*** shows, it took Spain, for example, 30 days on average to transmit fingerprints in Eurodac in 2017. This means that a person apprehended during an irregular border crossing into Spain had on average 30 days to reach another Member State and apply for asylum there. Authorities in that other country checking the fingerprints against the data in Eurodac would not have found any matches. Consequently, the other country would have been obliged to process the person's asylum application.

# Conclusions and recommendations

**83** We examined whether the EU information systems for internal security support border control efficiently. We concluded that border guards are increasingly using and relying on these systems when performing border checks. However, some data is currently not included in the systems, while other data is not complete or not entered in a timely manner. This reduces the efficiency of some border checks.

**84** We found that the EU information systems were generally well designed to facilitate border checks. The countries we visited have set up their systems in line with the applicable legal framework. Nevertheless, some national SIS II and VIS components facilitated more efficient border checks than others (see paragraphs ***17***-***21***).

**85** While Member States are sharing more and more information via the systems, legal constraints (data protection and national security rules) prevent sharing of human resources. Border guards visiting other Member States cannot access their host countries' information systems to perform border checks. We also noted that the systems were set up without a training environment in which border guards could practise scenarios that they do not encounter frequently on the job (see paragraphs ***22***-***23***).

## Recommendation 1 – Promote the use of SIS II and VIS training environments

The Commission should promote the use by the Member States of the central SIS II and VIS training environments, which would allow border guards to experience real life situations during their training.

**Timeframe: end of 2020.**

**86** The implementation of IT solutions was sometimes delayed, both at EU and national level. Four years after the Eurosur regulation entered into force, only half of the Member States were sharing all obligatory and voluntary information on the Eurosur platform. Fourteen countries failed to implement the rules on Passenger Name Record data on time. This prevented border authorities from having a full picture of the situation at the external borders of the Schengen area as well as advance information about high-risk individuals crossing them (see paragraphs ***24***-***32***).

**87** The Schengen evaluation mechanism plays an important role in monitoring the Schengen States' compliance with Schengen rules. We found that these evaluations were generally thorough and methodical, and addressed key aspects of the systems. However, it takes a long time for the Schengen States to remedy weaknesses identified during the evaluations. This is due to a lack of deadlines for the adoption of evaluation reports and the implementation of corrective action plans (see paragraphs ***33***-***41***).

**88** The Commission has not met its obligation to report annually to the Parliament and the Council on the evaluations carried out. We found that up to four years after their evaluations, none of the Schengen States covered by the audit had fully implemented their action plans. This shows that the evaluation process does not swiftly remedy identified weaknesses (see paragraphs ***42***-***43***).

## Recommendation 2 – Speed up the correction of weaknesses detected during Schengen evaluations

The Commission should:

(a) when presenting the evaluation report provided for under Article 22 of Regulation 1053/2013 to the Parliament and the Council, include information on the delays encountered by the evaluated Schengen States' implementation of their action plans to address the Council recommendations.

(b) propose appropriate legislative and procedural measures in order to shorten the timeframe of the Schengen evaluation cycle.

**Timeframe: end of 2020.**

**89** The EU provides Member States with funding from the Internal Security Fund for the development and maintenance of the information systems covered by our audit. On average, the countries we visited dedicated 15 % of their Internal Security Fund allocations to these five systems. They mostly used this EU money for maintenance of SIS II and VIS and extensions of Eurosur and PNR (see paragraphs ***44***-***46***).

**90** We found that the Member States are making increasing use of the systems. Between 2013 and 2017, the number of hits in SIS II relating to wanted persons and objects based on alerts originating in other countries almost tripled (see paragraphs ***47***-***58***).

**91** However, this use could be more systematic. Our survey reveals that more than half of the border guards had been in a situation where they had to decide whether to let someone through without consulting the systems. In particular, we noted a discrepancy between the number of visas issued and the number of visas checked. Moreover, VIS can only handle short-term Schengen visas – it is not currently designed to accommodate data on national visas, which also allow holders to enter any Schengen State. In 2017 alone, almost 2.6 million such visas were issued (see paragraphs ***59***-***62***).The Commission has identified this information gap and has tabled a proposal to revise the VIS legal framework.

## Recommendation 3 – Analyse discrepancies in visa checks

The Commission should analyse the reasons for discrepancies between the number of Schengen visas issued and the number checked, and propose corrective measures.

**Timeframe: end of 2020.**

**92** Border guards use the data in the systems as their basis for making decisions that affect the safety of European citizens. The quality of this data is therefore of the utmost importance. We found little reference to the issue of data quality in the legal acts governing the European information systems. The SIS II regulation gave Member States the responsibility for data quality and did not involve the Commission or eu-LISA (see paragraphs ***63***-***65***).

**93** Although eu-LISA performs automated monthly quality checks on the data in SIS II and transmit the results to the countries concerned, the agency can only see the aggregate numbers of quality issues for each type of alert and each country. This report is not sufficiently detailed to see the progress made in addressing data quality issues. Furthermore, neither eu-LISA nor the Commission have any enforcement powers to ensure that Schengen countries correct data quality issues in a timely manner (see paragraphs ***67***-***70***).

**94** We found that border guards do not always get timely and complete data from the information systems, which undermines the efficiency of border checks. For example, when border guards check a name in SIS II, they may receive hundreds of results (mostly false positives), which they have to check manually. This not only makes border checks less efficient, but also increases the risk of real hits being overlooked (see paragraphs ***71***-***76***).

## Recommendation 4 – Improve data quality control procedures

The Commission should:

(a) ask eu-LISA to include, in its monthly monitoring, statistics on corrections made by the Schengen States.

(b) if data quality monitoring does not indicate improvement take the necessary steps, e.g. via guidance or existing advisory groups, to encourage Schengen states to step up their corrective actions.

**Timeframe: by the end of 2020.**

**95** Except in the case of Eurodac, there are generally no compulsory deadlines on entering data. For example, Eurosur is meant to provide real-time information on the situation at the external borders. However, while some of the countries covered by our audit do indeed enter information in Eurosur on a real-time basis, others do so only once a week. Since Eurodac started operating in 2003, there has not been a single year in which all Member States have transmitted the required information on time. Delayed transmission can lead to the wrong country being designated responsible for processing an asylum application (see paragraphs ***77***-***82***).

## Recommendation 5 – Reduce delays in data entry

The Commission should:

(a) analyse the causes of irregular delays in Eurodac data entries and take appropriate action towards the Member States concerned.

(b) propose during the next revision of the applicable legislation for Eurosur that binding deadlines on data entry are introduced.

**Timeframe: end 2021.**

This Report was adopted by Chamber III, headed by Ms Bettina JAKOBSEN, Member of the Court of Auditors, in Luxembourg at its meeting of 8 October 2019.

*For the Court of Auditors*

Klaus-Heiner Lehne
*President*

# Annex

## Brief description of the information systems selected

### SIS II

The Schengen Information System (SIS) is the most widely used and largest information sharing system for security and border management in Europe. SIS II enables competent national authorities, such as the police and border guards, to enter and consult alerts on persons or objects. A SIS alert does not only contain information about a particular person or object but also instructions for the authorities on what to do when the person or object has been found.

SIS II consists of three major components: a central system, the national systems and a communication infrastructure (network) between the systems. An alert entered in SIS II in one Schengen State is transferred in real time to the central system. It then becomes available in all the other Schengen States.

Each Schengen State using SIS II is responsible for setting up, operating and maintaining its national system and its national SIRENE Bureau, which serves as a single point of contact for the exchange of supplementary information and coordination of activities related to SIS II alerts.

The EU Agency for large-scale Information systems (eu-LISA) is responsible for the operational management of the central system and the communication infrastructure.

The European Commission is responsible for the general supervision and evaluation of the system and for the adoption of implementing measures.

SIS II is in operation in 30 European countries, including 26 EU Member States (only Ireland and Cyprus are not yet connected to SIS II) and 4 Schengen Associated Countries (Switzerland, Norway, Liechtenstein and Iceland).

### VIS

The Visa Information System (VIS) supports the implementation of the common EU visa policy. It allows Schengen States to exchange visa data. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

VIS enables border guards to verify that the person presenting a visa is its rightful holder, that the visa is authentic and that the person still meets the visa requirements.

A digital photograph and 10 fingerprints are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database. Using biometric data to confirm a visa holder's identity allows for faster, more accurate and more secure checks. The system also facilitates the visa issuance process.

VIS consists of a central IT system and of a communication infrastructure that links the central system to national systems. VIS connects consulates in non-EU countries and all external border checkpoints of Schengen States. It processes and stores data and decisions relating to applications for short-stay visas.

As a Schengen instrument, VIS applies to all Schengen Area countries. The EU Agency for large-scale Information systems, eu-LISA, is responsible for the operational management of VIS.

## Eurodac

EURODAC is an EU asylum fingerprint database. Its primary objective is to serve the implementation of Regulation (EU) No. 604/2013 ('the Dublin regulation'). When someone applies for asylum, no matter where they are in the EU, their fingerprints are transmitted to the EURODAC central system.

Since it was established in 2003, EURODAC assists with determining the Member State responsible for processing an asylum application.

EURODAC contains only fingerprints (along with data and place of registration) but no other personal information. The countries using the system are the 28 EU Member States and Schengen Associated countries: Iceland, Liechtenstein, Norway and Switzerland.

## Eurosur

The European Border Surveillance system (EUROSUR) sets up a governance framework for cooperation between the Member States and **EBCGA (“Frontex”)** in order to improve European situational awareness and increase reaction capability at the external borders. The aim is to prevent cross-border crime and irregular migration and contribute to protecting migrants' lives.

Under the Eurosur Regulation, each Schengen State has a National Coordination Centre (NCC) which coordinates and exchanges information among all the authorities responsible for external border surveillance as well as with other NCCs and Frontex.

Frontex is responsible for coordinating the so-called common application of surveillance tools: the Member States can request Frontex' assistance in monitoring selected areas or vessels of interest for Eurosur purposes by using tools like satellite imagery or ship reporting systems. This can be used to detect cases of irregular migration or cross-border crime, but also to locate a boat in distress.

Eurosur is used in all Schengen area countries, as well as Bulgaria, Romania and Croatia.

### PNR

Passenger Name Record describes information provided by passengers to airlines when making reservations and carrying out the check-in process. It may contain information, such as dates of travel, travel itinerary, ticket information, contact details, travel agent, means of payment, seat number and baggage information. On 27 April 2016, the European Parliament and the Council adopted the Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

All EU Member States, apart from Denmark[28] are required to establish specific entities responsible for the collection, storage and processing of PNR data, the Passenger Information Units (PIUs). The PIUs collect the PNR data from air carriers using a dedicated IT system and compare PNR data against relevant law enforcement databases. They also process them against pre-determined criteria, in order to identify persons that may be involved in a terrorist offence or serious crime. The PIUs are also in charge of disseminating PNR data to border guards and other national competent authorities, Europol and PIUs of other Member States.

[28] On the basis of Protocol 22 to the Treaties Denmark does not participate in the PNR Directive.

# Acronyms and abbreviations

**DG HOME:** Directorate-General for Migration and Home Affairs

**EBCG:** European Border and Coast Guard Agency

**eu-LISA:** European Agency for the operational management of Large-Scale Information systems in the area of freedom, security and justice

**Eurodac:** European Dactyloscopy

**Eurosur:** European Border Surveillance System

**Frontex:** *see EBCG*

**ISF:** Internal Security Fund

**NCC:** National Coordination Center

**PNR:** Passenger Name Record

**SIS II:** Schengen Information System II

**VIS:** Visa Information System

# Glossary

**Border checkpoint:** any crossing-point authorised by the competent authorities for the crossing of external borders.

**Border guard:** any public official assigned, in accordance with national law, to a border checkpoint or along the border or the immediate vicinity of that border who carries out border control tasks.

**First-line:** location at which all persons are checked at the border checkpoint.

**Interoperability:** interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged.

**Second line check:** a further check which may be carried out in a special location away from the location at which all persons are checked (first line).

**Schengen area countries:** 26 European countries that have eliminated all passport controls on their common borders, of which 22 are EU Member States and 4 are EFTA countries: Belgium, Czech Republic, Denmark, Germany, Estonia, Greece, Spain, France, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Slovenia, Slovakia, Finland, Sweden, Iceland, Liechtenstein, Norway, Switzerland.

**Schengen Associates states:** four European Free Trade Association (EFTA) member states (Iceland, Liechtenstein, Norway, and Switzerland), which are not members of the EU, but have signed agreements in association with the Schengen Agreement.

**REPLIES OF THE COMMISSION TO THE SPECIAL REPORT OF THE EUROPEAN COURT OF AUDITORS**

**"EU INFORMATION SYSTEMS SUPPORTING BORDER CONTROL – A STRONG TOOL, BUT MORE FOCUS NEEDED ON TIMELY AND COMPLETE DATA"**

## EXECUTIVE SUMMARY

II It is important to underline that Passenger Name Record (PNR) data collected under the PNR Directive cannot be used for border/immigration control purposes, but only for law enforcement purposes in combatting serious crime and terrorism.

VI The deadline for the transposition of the PNR Directive passed on 25 May 2018. Therefore, it is a relatively new instrument, in comparison with other systems covered by the ECA's audit.

Member States are required to equip their Passenger Information Units with hardware and software for the collection and processing of PNR data. To establish connectivity with an air carrier is a lengthy and complicated process, which does not depend entirely on national authorities. Moreover, PNR data cannot be collected and processed without a legal basis (i.e. before national transposing measures have been adopted and entered into force). All these factors explain why it may take time before national Passenger Information Units become fully operational. The Commission has assisted Member States along the implementation process, including by making EU funding available for the acquisition and development of the necessary hardware and software.

The Commission does not consider that there were long delays in the implementation of IT solutions for Eurosur.

The Eurosur communication network, interlinking the Member States' national coordination centres for border surveillance with each other and with the European Border and Coast Guard Agency (Frontex) has been established in time, allowing for instance to exchange information on incidents related to irregular migration and cross-border crime.

However, there has indeed been a delay in finalising the accreditation process for the exchange of some information due to confidentiality requirements.

VII The Commission agrees with the ECA that concrete and binding deadlines for the implementation of the recommendations by the concerned Member States would considerably strengthen the efficiency of the Schengen evaluation mechanism and close the identified gaps more swiftly.

Concerning the time period for the adoption of the evaluation reports, the Commission is looking into possible procedural changes to shorten this time period.

VIII With the ever-increasing passenger flow, it is important to invest in solutions that enable a systematic check in all relevant systems for all passengers, regardless of the particular situation or passenger queue.

IX As regards the Commission's enforcement powers, the Commission is responsible for monitoring the correct implementation of EU legislation by Member States. Therefore, although the Commission does not have access to SIS data and cannot assess individual cases, it can verify that the structures and mechanisms are in place at national level to ensure high quality of data in SIS.

X In relation to data in SIS, there is an agreed set of mandatory data without which an alert cannot be created (therefore any alert is SIS is always complete) but there is also data which would only be there if available or if considered safe to include by the issuing authorities. Supplementary information may also be available at SIRENE office. End-users are always instructed in the alert to contact their national SIRENE office (in some cases immediately).

Regarding VIS and false positives, VIS as a general rule contains biometric data (10 good quality fingerprints), so provided that the checks are properly done (fingerprints of a person), this means that false positives are not an issue for VIS. Furthermore, the findings of the 2016 REFIT of VIS show that data quality, including for biometrics, is very good in VIS.

XI In its 2018 Eurosur evaluation report the Commission has also highlighted the different timeliness of Member States in inserting information into Eurosur. This issue has therefore been addressed in the new European Border and Coast Guard Regulation (which now also includes Eurosur), allowing to agree on binding implementing rules on the Eurosur information exchange in the future.

XII The Commission accepts the recommendations.

## INTRODUCTION

03 The Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and persecution of terrorist offences and serious crime, known as PNR Directive does not create a centralised IT system at EU level. Each Member State has its own Passenger Information Unit (PIU), which collects, process and store PNR data. National PIUs of Member States may transfer or request PNR data from PIUs of other Member States in accordance with procedures set in Article 9 of the PNR Directive.

Eurosur is not a specific information system comparable to SIS VIS or PNR but a "common framework for the exchange of information and for the cooperation between Member States" and the European Border and Coast Guard Agency (Frontex). Data in Eurosur can be collected by different information systems.

## OBSERVATIONS

20 The national components of SIS II and VIS are under Member States responsibility.

24 Eurosur is providing a framework not only for information exchange, but also for cooperation, with different components. The Eurosur communication network has been established in time, interlinking all participating Member States in 2013/2014 with each other and with the European Border and Coast Guard Agency (Frontex). However, there have been some delays in finalising the accreditation of the Eurosur communication network as far as the exchange of classified information is concerned.

27 The security accreditation for the exchange of classified information in the Eurosur communication network has been delayed, but it should be noted that this kind of information covers only a very small part of the information being exchanged.

28 The Commission has continuously supported Member States in the implementation and application process via funding, assistance, facilitating peer-to-peer exchange via organisation of regular meetings and workshop and providing training (mostly via CEPOL).

29. The Netherlands and Finland have in the meantime notified full transposition of the PNR Directive (Finland on 25 June 2019 and the Netherlands on 8 July 2019).

30 Establishing connectivity with airlines is a technically complex and lengthy process which may take up to 6-9 months for each airlines. It involves companies which provide reservation services to airlines. The demands to connect air carriers to PIUs have grown in numbers since the adoption of the PNR Directive.

It should also be noted that since March 2019 many Member States have made very significant progress regarding the connectivity process.

31 The system is relatively new and is still at the implementation phase.

PNR data is not only cross-checked with data bases but may also be checked against pre-established targeting rules to identify passengers who correspond to certain profiles, based on the intelligence available.

This technique allows to identify individuals unknown to authorities, but involved in illegal activities such as terrorism or trafficking.

32 PNR data may only be used to combat terrorism and serious crime as defined in the PNR Directive. The scope of SIS legislation is broader (for example alerts may be introduced in cases of crimes which are not covered by the PNR Directive).

PNR data is data provided by passengers when they book their flights. For intra-EU flights it does not contain API data (i.e. data from official ID documents, such as date of birth; date of birth is crucial in the identification of persons). Therefore, PNR data is both unverified and incomplete from law enforcement point of view.

Air carriers transfer data of all passengers. To compare this data with databases and targeted rules allows to identify known or unknown suspects.

SIS II is one of the databases used by national authorities in the processing of PNR data.

40 Besides regular visits, there are also several unannounced evaluations each year. During these visits, it is possible to assess the implementation of the previous recommendations. There has been one unannounced visit and four re-visits concerning SIS II.

41 The Commission organises a revisit with the specific aim to assess the implementation of the previous recommendations.

Box 2 – Hitting the right target

It should be noted that a match in SIS occurs when a search reveals the existence of an alert issued by another Member State (the result of an automated search). A list of potential "matches" is displayed to the end-user (for example, the border guard) who needs to verify the match. There is always a manual verification, as is required by EU data protection law. Only following the manual verification, the match is confirmed and becomes a so-called hit.

58 This issue has been addressed in the new European Border and Coast Guard Regulation which will enter into force later this year and which will repeal the current Eurosur Regulation.

In particular the EBCG Agency will monitor the data exchanged and will inform all Member States in real time on the status of reporting.

The reporting on Border Crossing Points will become compulsory.

61 Using VIS to check visa holders at the border is an obligation stemming from Schengen borders code. The Schengen evaluation mechanism could be used to analyse this possible discrepancy to ensure that visas are systematically checked against VIS.

68 These are potential issues that need to be crosschecked by the responsible authority, and not confirmed data quality errors. In addition, it should be noted that the number also includes all alerts that have already been verified by the Member States and for which it is confirmed that they do not represent a data quality issue. These verified alerts are not removed from the detailed report but stay in the report as long as the alert exists.

71 The SIS legislation defines the set of data that may be entered in the alert (common Article 20 of the SIS II Decision and SIS II Regulation). Data minimisation is an important principle of data protection. In addition, the legislation also lays down the minimum set of data, without which no alert can be created. Therefore, any alert containing those minimum data elements is a complete alert. Other (optional) data elements should be entered, when available. In case such optional data is not entered, the Commission can only assume that the data is not available to the issuing authority.

72 The obligation to carry out a manual verification is a requirement of EU data protection legislation (General Data Protection Regulation (Regulation (EU) 2016/679) and Police Directive on data protection (Directive (EU) 2016/680)). In addition, it is a requirement under the PNR Directive.

Most PNR data is insufficient, irrelevant and sometimes too unreliable for SIS check purposes e.g., PNR data without API values can only be checked against a very limited set of SIS data. Moreover, the fact that PNR data are based on self-declaration raises issues of reliability.

74 The ECA rightly points out that the Commission's proposal to revise the VIS legal framework (COM (2018) 302), currently being discussed by the co-legislators, provides for the inclusion of national visas and residence permits in VIS. The information gap referred to by the ECA would thus be closed. While it is true that only newly issued long-stay documents would be included, this is an issue that would disappear over time as long-stay documents have a limited validity period and have to be renewed/ replaced.

75 The issue of different formats of the reports submitted by Member States has been addressed in the new European Border and Coast Guard Regulation which is expected to enter into force by the end of 2019 and which will repeal the current Eurosur Regulation.

The reporting in Eurosur will be standardised via an implementing act.

76 See the Commission reply to paragraph 75.

In addition, the Commission will support the development of automated information exchange gateways to limit double data inputs.

79 The issue of timing for reporting of Member States in the framework of Eurosur has been addressed in the new European Border and Coast Guard Regulation, which is expected to enter into force by the end of 2019 and which will repeal the current Eurosur Regulation.

The implementing act on Eurosur will address the timing for reporting information in Eurosur as well as the level of responsibility for reporting.

## CONCLUSIONS AND RECOMMENDATIONS

84 The national components of SIS II and VIS are under Member States responsibility.

85 Commission, Member States, CEPOL and eu-LISA have ensured regular common training for SIRENE officers in the field of SIS II/SIRENE. A training needs analysis has also been carried out.

Member States are increasingly considering investing in integrated/online hands-on training environments.

The amended legislation establishing the relevant IT systems (e.g. SIS II) will provide for the possibility of the EBCG Agency (Frontex) developing specific interfaces suitable for use by the guest officers deployed in any Member States.

**Recommendation 1 – Promote the use of SIS II and VIS training environments**

The Commission accepts recommendation 1.

86 Concerning Eurosur, it should be noted that only part of the information being exchanged is compulsory. For instance, there is the possibility but no obligation for Member States without external land and sea borders to exchange information concerning air borders. However, with the new European Border and Coast Guard Regulation, border checks and air border surveillance have also been included in Eurosur (as an obligation), meaning that in the future almost all Member States will actively provide information in Eurosur.

See Commission replies to paragraphs 24-32.

**Recommendation 2 – Speed up the correction of weaknesses detected during Schengen evaluations**

The Commission accepts recommendation 2.

**Recommendation 3 – Analyse discrepancies in visa checks**

The Commission accepts recommendation 3.

**Recommendation 4 – Improve data quality control procedures**

The Commission accepts recommendation 4.

The Commission and eu-LISA are currently already in the process of improving the mechanism. The point is regularly addressed in the SIS-VIS Committee.

95 The issue of timing for reporting information has been addressed in the new European Border and Coast Guard Regulation which is expected to enter into force by the end of 2019 and which will repeal the current Eurosur Regulation. The implementing act on Eurosur will address the timing for reporting information in Eurosur as well as the level of responsibility for reporting.

**Recommendation 5 – Reduce delays in data entry**

The Commission accepts recommendation 5 (a).

The Commission accepts recommendation 5 (b).

The Commission agrees with the part concerning Eurosur. The issue of deadlines on data entry has been addressed in the new European Border and Coast Guard Regulation which is expected to enter into force by the end of 2019, which will repeal the current Eurosur Regulation and which will allow to agree on binding implementing rules on the Eurosur information exchange in the future.

# Audit team

The ECA's special reports set out the results of its audits of EU policies and programmes, or of management-related topics from specific budgetary areas. The ECA selects and designs these audit tasks to be of maximum impact by considering the risks to performance or compliance, the level of income or spending involved, forthcoming developments and political and public interest.

This performance audit was carried out by Audit Chamber III External action/Security and justice, headed and led by ECA Member Bettina Jakobsen, supported by Katja Mattfolk, Head of Private Office and Kim Storup, Private Office Attaché; Alejandro Ballester Gallardo, Principal Manager; Piotr Senator, Alexandre Tan and Mirko Iaconisi, Auditors. Michael Pyper provided linguistic support.

*From left to right:* Mirko Iaconisi, Piotr Senator, Michael Pyper, Bettina Jakobsen, Alejandro Ballester Gallardo, Katja Mattfolk.

# Timeline

| Event | Date |
|---|---|
| Adoption of Audit Planning Memorandum (APM) / Start of audit | 17.4.2018 |
| Official sending of draft report to Commission<br>(or other auditee) | 11.7.2019 |
| Adoption of the final report after the adversarial procedure | 8.10.2019 |
| Commission's (or other auditee's) official replies received in all languages | 31.10.2019 |

| | | | | |
|---|---|---|---|---|
| EN | PDF | ISBN 978-92-847-3858-8 | doi:10.2865/83092 | QJ-AB-19-020-EN-N |
| EN | HTML | ISBN 978-92-847-3824-3 | doi:10.2865/695262 | QJ-AB-19-020-EN-Q |

The abolishment of border checks at the internal Schengen borders reinforced the importance of effective control and surveillance of the Schengen area external borders. To help border guards control these, the EU has set up a number of information systems. Our audit examined whether the main
EU information systems for internal security support border controls efficiently. We found that border guards are increasingly using and relying on the systems when performing border checks. However, some data is currently not included in the systems, while other data is either not complete or not entered in a timely manner. This reduces the efficiency of some border checks. We make a number of recommendations, e.g. that data quality procedures are improved and that delays in data entries and the time taken
to correct identified weaknesses are reduced.

ECA special report pursuant to Article 287(4), second subparagraph, TFEU.

EUROPEAN COURT OF AUDITORS

Publications Office

EUROPEAN COURT OF AUDITORS
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Enquiries: eca.europa.eu/en/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors