SIS II Supervision Coordination Group

Activity Report

2013-2015

Contents

Foreword

We are pleased to present the Activity Report covering the period 2013 to 2015. This is the first report under the new legal framework and also with the new supervision structure, comprising of the Data Protection Authorities (DPAs) and the European Data Protection Supervisor (EDPS), both exercising their respective roles and coordinating activities within the newly formed SIS II Supervision Coordination Group (SIS II SCG).

The first two years of activities of the SIS II SCG were both motivating and challenging for a number of reasons.

Primarily the group had a sense of responsibility to guarantee that an effective system of supervision is maintained in practice, also by ensuring that the work and data protection legacy of its predecessor (the former JSA Schengen) is properly inherited and conserved. DPAs play a major role in this, given that they have been part of the former supervision platform since its inception. Over twenty years of experiences and achievements, all with the main objective of upholding the data protection rights of individuals.

On a practical level, one of the major challenges is posed by the new legal framework and the novelties brought up with it. Significant changes with impact to data protection include additional data categories and linking functionalities in the system, the mandatory audit requirement and also specific time frames for the exercise of data subjects' rights. The SIS II SCG has a clear mission to ensure a smooth transition to the new legal basis and a consistent approach by DPA's in dealing with SIS II.

In the period covered by this report, the Group was also faced by an unprecedented challenge in the field – the Danish N-SIS hacking incident, which resulted in personal data from the SIS being compromised, required action by DPA's not only to guarantee the security and integrity of the personal data processed in SIS but also to restore trust and reassure data subjects that their rights are being defended. We will endeavour to continue our mission in this direction.

Clara Guerra

Chair

David Cauchi

Vice-Chair

Introduction

The second generation of the Schengen Information System (SIS II) went operational from 9 April 2013 and is regulated by Regulation (EC) 1987/2006[1] (hereinafter "the SIS II Regulation") and Council Decision 2007/533/JHA[2] (hereinafter "the SIS II Decision").

According to the new SIS legal framework, supervision over the N.SIS II is allocated to the Data Protection Authorities (DPAs) in the respective Member State while the Management Authority (eu-LISA), responsible for the operational management of the Central SIS II, is supervised by the European Data Protection Supervisor (EDPS).

To ensure coordinated supervision of the SIS II, the national DPAs and the EDPS shall cooperate actively in the framework of their responsibilities, by exchanging relevant information, assisting each other in carrying out audits and inspections, examining difficulties of interpretation or application of the SIS II Regulation and Decision, drawing up harmonised proposals for joint solutions to any problems, promoting awareness of data protection rights, studying problems in the exercise of the rights of the data subjects[3].

For these purposes, the SIS II legal framework provides that national DPAs and the EDPS shall meet at least twice a year, adopt rules of procedure and develop further working methods as necessary.

The SIS II Supervision Coordination Group (SIS II SCG) was then set up on 11 June 2013, when its first meeting took place.

The work of the Group started right away following the presentation by the Danish DPA about the very serious SIS national hacking incident, that had just been uncovered and whose consequences were still to be known. This was clearly an issue that required a common action from the supervisors, as this kind of breach affects all Member States and compromises the security of personal data.

This Report accounts for the activities undertaken by the SIS SCG from 2013 to 2015. According to Article 12.1 of the Rules of Procedure, it also includes a part dedicated

[1] Regulation (EC) 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 (JOL 381, 28.12.2006).
[2] Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (JOL 205, 7.8.2007).
[3] According respectively to articles 46 and 62 of the SIS II Regulation and Decision.

to national reports prepared by the national DPAs and presented in a standard model.

These first two years of activity were intense and mostly focussed on the study of the Schengen new legal instruments and on the preparation of a common audit framework to assist DPAs to perform their inspective role while allowing comparable results.

During this period, the development of relevant data protection awareness initiatives was a key activity of the SIS II Group as well.

Furthermore, within the recent context of coordinated supervision, the SIS II Group actively contributed to create synergies with other SCGs, in particular those with evident links to Schengen matters, such as VIS and EURODAC, by promoting whenever possible a horizontal approach in developing activities.

Currently the SIS II SCG is composed of 30 members[4] and 3 observers[5]. This is indeed a significant platform to promote cooperation, to share experiences and exchange perspectives, to give opinions and find solutions, i.e. to improve supervision. And data protection supervision is vital to guarantee the rights of the individuals. That is our task and we will carry it through.

[4] Twenty-nine members representing the DPAs of the Member States, these considered as the ones participating in the SIS, and the EDPS.
[5] Croatia, Cyprus and Ireland.

Part I – The Supervision Coordination Activity

During this period, the SIS II SCG organized 6 (six) meetings[6], all taking place in Brussels, and supported by the Secretariat provided by the EDPS.

The rules of procedures were adopted in the first meeting and, based on priorities ranked by delegations, a working program for the years 2013-2015 was adopted in the second meeting, guiding not only the Group's activity for the last two years, but its working methods as well.

A. Working methods

The SIS II SCG decided to use flexible mechanisms to carry on its work while ensuring a high level of participation and involvement of all its members.

Taking into consideration the workload of DPAs and some financial and human resources restraints, the SIS II SCG tried to rationalize as far as possible the organisation of its work; therefore the meetings were organised, whenever possible, back to back with the VIS and EURODAC SCGs, taking advantage of the common membership of these groups in most of the cases.

On the other hand, due to the current interaction between the large information systems, in the borders' context, the SIS II SCG explored some synergies with the VIS and EURODAC SCGs, avoiding duplication of work at the same time as improving the consistency of data protection supervision.

Likewise, cooperation can be extended, as needed, to the Joint Supervisory Body (JSB) Europol and JSB Eurojust, by sharing relevant information related to the access by Europol and Eurojust to the data in SIS II. It already happened with the JSB Europol, as described below.

In order to develop work in a more efficient way, the SIS II Group established 4 subgroups to handle specific tasks or prepare its position on certain matters, without prejudice of the continuous guidance and follow-up provided by the plenary: IT expert subgroup; Alerts subgroup; Alert deletion on stolen cars subgroup and Website subgroup.

To promote cooperation and enhance communication within the Group, it was discussed with the EDPS the possibility of using the CIRCABC network as the basic tool for sharing information, supporting the meetings, archiving relevant

[6] June 2013, October 2013, May 2014, October 2014, March 2015, October 2015.

documents, organising subgroups work or using the directory functionality to communicate in a secure, fast and costless way.

B. Main activities

The SIS II SCG succeeded in fulfilling most of the activities proposed for its bi-annual working program, although a few have not been completed yet; likely they will be finished in the first half of 2016.

On the other hand, as the work is not limited to planned activities, the Group had to deal with some emergent questions that required its engagement in discussing and taking position.

1. Follow-up Danish hacking incident

The SIS II SCG pursued the Danish incident from the very beginning, when in its first meeting the Director of the Danish DPA reported the hacking of the Danish N.SIS; the facts known at that moment, although still not complete, already gave a clear indication of the extent of the breach and of the need for all DPAs be involved and be kept informed. This was not merely a security breach but also a privacy breach.

Therefore, it was decided to set up an IT expert's subgroup to follow-up this issue and liaise with the Commission efforts' to check the security of the whole system. The Group addressed the Commission highlighting the need to be involved, considering its legal competences of ensuring coordinated supervision of the SIS II both at national and EU level. A representative of the SIS SCG participated in a couple of meetings of the working group led by the Commission to make an end-to-end security assessment of the SIS. Out of that work some general recommendations were made in early 2014.

Meanwhile, in a coordinated initiative of the SIS II Group, all national DPAs took action at national level and approached their respective national competent authorities regarding eventual consequences of the Danish incident and whether assessments or monitoring of potential risks were envisaged.

The transition process from SIS I to SIS II was also addressed by national DPAs, that requested information about the general functioning of the new system and the procedures for termination the old one, in particular the deletion of data stored in N.SIS I.

Apart from the specific monitoring performed at national level, feedback from this activity was given by delegations and information was exchanged within the Group, allowing to have a general perspective of events and practices.

The Danish DPA proactively shared with the SIS II SCG the findings of its own investigation and its decision. Being this a rather important topic, the Group had discussed this issue several times in the last two years to mainly conclude that security should be a priority for MS and that national competent authorities must have an effective control of the data, in particular when processing activities are outsourced.

2. Report on the Right of Access

The SIS II SCG took this activity from the former Schengen JSA, who started this report based on a questionnaire on how the rights of the data subjects were exercised in MS, according to national law: form of access, statistical data on requests (access, correction, deletion and checks); communication to the data subject and cooperation with other Schengen States.

The information collected through this questionnaire was quite relevant to have an overview of national practices, to assess their legal compliance and to evaluate the cooperation procedures.

As the SIS II legal framework did not impact in this activity, the Group completed it assembling the remaining answers, and drafted a final report on the findings. First of all, the difficulty of collecting statistics and comparable data demands for a common approach in this area. The report also signals a couple of significant shortcomings in providing the access to the data subjects, mostly in terms of deficient cooperation between MS. The Report makes some recommendations both to competent authorities and to national DPAs.

3. Development of a common audit framework

According to the SIS II Regulation and Decision[7], national DPAs and the EDPS have to carry out an audit every four years using international auditing standards. The same obligation applies to the VIS and to the EURODAC systems.

In order to assist the DPAs in performing this legal obligation until 2017, the SIS SCG decided to develop a common audit framework as a valuable tool for inspections

[7] Articles 44 and 45 of the Regulation and articles 60 and 61 of the Decision.

while enabling a better comparison of results. On the other hand, this will bring more consistency to the supervision.

This audit framework was divided in two complementary parts: a security module and an alert module, each one handled by different subgroups. The security module focuses on security aspects and follows the auditing international standards. The work was finalised in 2015 by the IT subgroup and it is ready to be used by DPAs. Moreover, this was an activity benefiting from a horizontal approach, so the development of this module can also be applied to VIS and EURODAC systems.

The alert module explores the rules concerning the alerts, such as categories of data processed, conditions for insertion, retention periods and their review, links between alerts, misused identity, and so forth. This exercise entails a more legal approach, and it will function as a checklist for inspecting the alerts. This work was almost completed in 2015, but still lacking a final revision for adoption in the first half of 2016.

Both modules create a comprehensive framework for auditing the SIS II and constitute definitely a key activity of this two-year period. It is now possible to build on this solid ground to enlarge the scope of the framework to other components of the SIS, like the users of the SIS.

For that purpose, The Group took on another activity, based on a fact finding questionnaire, to have an overview on access to the SIS II. The intention was to find out how the access is being performed. The replies were all collected and the draft report is now under discussion. The conclusions may lead to further action.

4. Interpretation and application of the legal framework

One of the legal tasks assigned to this Group is to examine difficulties of interpretation or application of the SIS II Regulation or of the SIS II Decision.

The intervention of the SIS II SCG in this respect comes often from requests of national DPAs, but actually it does not have to be necessarily so. The great experience and expertise in Schengen matters combined together in this Group brings out the usefulness and efficacy of providing advice for other stakeholders if necessary.

a. Systematic checks in the SIS II of hotel guests lists

The Group analyzed a request from the Swiss DPA on the legal compliance of the systematic verification (100% cross-checks) in the Schengen Information System of

national hotel guests' registers and whether the new legal framework changed the assessment formerly made by the Schengen JSA under the Schengen Convention.

The JSA had at that time considered that the procedure carried out by the Swiss authorities was not in compliance with Articles 45 and 112 of the Schengen Convention for deviation of the purpose limitation. In spite of the possibility afforded to national law to give the data a different use, the JSA concluded that it would only be legitimate in that case if in compliance with the purpose of the alert, necessary and proportionate. To perform a 100% verification is not, in any case, appropriate.

Though Article 45 is still in force, the SIS SCG assessed the other similar Articles in the SIS II legal framework and concluded that the opinion of the JSA remains valid under the new legal requirements. The new provisions do not differ in substance from the ones of the CISA, and in some extent the principle of purpose limitation is reinforced. Additionally, the SIS II SCG evoked the judgement of the CJEU of 8 April 2014 on the data retention directive[8], which enshrines this principle when recalling that the interference with the right to respect for private life should be limited to what is strictly necessary.

b. Access to SIS II under the Europol new logging system

The JSB Europol addressed the SIS II SCG with a request for interpretation of Article 41(5)(b) of the SIS II Decision prohibiting connecting parts of SIS II with Europol, in view of plans under discussion at Europol on a new logging system.

The Group discussed the matter but the lack of sufficient information, to evaluate whether the envisaged plans could constitute a practise admissible or excluded from the scope of the SIS II Decision, prevented it from taking a final position.

Nevertheless, the SIS II Group the SCG underlined that the prohibition of connecting parts of SIS II with Europol is of an intentionally restrictive nature. While flexibility might be granted on the basis of sufficient technical details and clarification of the purpose of such connection, a blanket exemption could however not be issued. So, the Group resolved to await further developments.

c. Alerts on stolen vehicles

The Group underwent a thorough exchange of views and information about the interpretation of Articles 38 and 39 of the SIS II Decision, after this matter being raised by a delegation.

[8] Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.

The case regards the circumstance when a stolen car, alerted to be used as evidence in criminal proceedings, is purchased in good faith in another MS; the car is located, the information is provided to the alerting MS but no following action is agreed; there is an impasse, the car is not returned, the alert is not deleted, the new owner cannot circulate abroad.

Bringing this issue for discussion, the SIS II SCG learnt that there are some MS having this problem and no satisfactory solution was yet found. The application of national law puts in evidence the differences between legal systems and practices and the SIS II legal framework does not provide a clear way out for the situation.

However, the SIS II Group is finalizing a common position on this issue, that most likely be taken during 2016.

5. Raising awareness of data protection rights

To promote awareness of data protection rights is decisive for their effective exercise by individuals. This is another of the SIS II SCG legal tasks and data protection authorities take this mission heartily.

The launch of the SIS II required straightaway that citizens were duly informed about the changes in the new legal framework, in particular those directly impacting on their data protection rights, such as the deadlines for receiving an answer after submission of a request for access, correction or deletion.

a. Guide of Access and update

For that reason, the SIS II SCG defined as its priority the compilation of a new Guide of Access[9], in line with the new legal framework, and enlarged with more Member States.

Besides a general presentation of the rights assisting individuals, this Guide contains detailed information by Member State on how to exercise the rights, contact details of competent authorities and of DPAs, requirements and procedures for submitting the request, national legal references, and also modal letters for exercising the right of access, correction or deletion.

The Guide was issued in English, in 2014, but translations of the first part of the document in all official languages were made available later on. The Guide was posted in the national DPAs and the EDPS website, and was referred to other

[9] The Schengen JSA had adopted, in 2009, a Guide of Access, which was no longer valid.

national bodies, including NGOs. It was distributed to the Parliament, the Council and the Commission for diffusion as well.

After being put into effect of the provisions of the Schengen *acquis* on data protection and of parts of the provisions on the SIS for the United Kingdom, the Guide of Access was in 2015 updated accordingly, now also comprising information of the UK.

b. SIS II European information campaign

The SIS II Group tried to follow-up the roll out of the SIS II European information campaign, at national level, since this action had been promoted by the Commission together with the competent authorities of the Member States, with no direct involvement of the DPAs.

The campaign included posters, leaflets and a video-animation. Through a coordinated initiative, national DPAs contacted the respective national competent authorities to enquire about the dissemination of the information materials. The DPAs also joined the campaign by uploading the materials in their websites.

c. Web archive of the Schengen JSA

The SIS II SCG was approached by the Council Data Protection Secretariat because of the expected suppression from the Council hosting services of the JSA Schengen website, what would put offline relevant documentation (opinions, inspection reports, activity reports, letters and so forth) of many years of activity. Consequently, much of the history of the first Joint Supervisory Authority would not be available to the public anymore; hence it would somehow be gone.

The Group agreed that a solution had to be found to prevent this loss and several scenarios were discussed. Finally, with the support and full commitment of the EDPS in leading this process, the contents of the Schengen JSA was successfully stored in the EU historical archive in Florence[10].

For benefit of experts, researchers and the general public, it is available online from 2015 a repository of information that constitutes a significant part of the Schengen heritage and of the European data protection legacy.

[10] http://collections.internetmemory.org/haeu/20150414150052/http://schengen.consilium.europa.eu/about/tasks-of-the-jsa-schengen.aspx?lang=en

d. Website for the Group

Still aiming to promote data protection, the SIS II SCG started to work together with the VIS and EURODAC SCGs in becoming more accessible to the public, thus likewise improving transparency, by means of having a website for the Group(s).

This will absolutely improve communication with the public and at the same time it will allow following-up the Group's activity. For that purpose a dedicated subgroup was set up to liaise with the EDPS services, which have been providing a great assistance in this regard, exploring possibilities and tabling proposals.

C. Institutional cooperation

The first level of institutional cooperation of the SIS II SCG is undoubtedly with the EDPS, not in the quality of member of the Group, but within the legal task and responsibility of providing the Secretariat to the Group and in bearing the costs of the meetings.

The coordinated supervision is a rather new context for all of us[11], especially in Schengen matters where a different model of supervision was in place. Consequently, it is of the utmost importance to keep a close and smooth cooperation to pave the way towards a high level of supervision, having always in mind our mission of guaranteeing the fundamental rights of the data subjects.

It should be highlighted that the cooperation with the EDPS has evolved in these first years of the Group in a positive course, reinforcing dialogue, trust and commitment among ourselves. This is essential to overcome any difficulties and to effectively ensure a coordinated supervision of the SIS.

The SIS II SCG also upheld, from the very beginning, a valuable cooperation with the Commission, by means of regular participation of its representatives (from DG HOME and DG JUST) in parts of the meetings to address any relevant matters while being available for Q&A with delegations.

As a privileged network to reach all national DPAs, the Commission began channeling through the Group the call for designation of experts for data protection evaluations, to get more easily experts in that area.

[11] A first ad-hoc experience was accomplished regarding the Eurodac system but yet informally, as it was not at that point legally framed. The CIS SCG started its activity in December 2010 and the VIS SCG in autumn 2012.

On the other hand, the Commission also invited the Group to a meeting of the SIS/VIS Committee that took place in March 2015 to present the report on the exercise of the right of access and the Guide of Access.

The SIS II SCG keeps a good working relation with the IT agency eu-LISA, as the Management Authority for SIS II, and invites to meetings a representative of the agency as needed.

At last, it should be noted the developing cooperation with the Fundamental Rights Agency (FRA) on a project about the use of biometrics.

Part II – The national activity

This Part provides an overview of the activity of the national DPAs as national supervisory authorities for the SIS II.

1. Austria

1. **Country**: Austria
2. **Name of the DPA**: Datenschutzbehörde
3. **Legal provisions implementing SIS II framework (short description)**:
   EU – Polizeikooperationsgesetz – Access by the Police
   § 33 Description
   § 34 Additional information
   § 35-40 Alerts
   § 41 Retention periods
   § 42 Rectification and deletion
   § 43 Right to access
   Justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (BGBl. I Nr. 36/2004)
   § 16 and 29 Access by Justice
4. **Number of complaints from data subjects**: 0
5. **Main issues object of complaints**: -
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: 0
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: 1
9. **Raising awareness activity**: 1
10. **Link for Schengen information in the DPA website**: http://www.dsb.gv.at/site/6192/default.aspx
11. **Any relevant case-law: -**
12. **Any other relevant activity: -**

2. Belgium

1. **Country**: Belgium
2. **Name of the DPA**: Commission for the protection of privacy (CPP)
3. **Legal provisions implementing SIS II framework (short description)**:
   - The Belgian Act on the office of police of 5 August 1992
     - This Act determines the general rules for the police information management.
   - The MFO 3 Common Guideline of the Federal Public Service of the Interior (FPSI) and the Federal Public Service of Justice (FPSJ) about information management relating to the judicial and administrative police
     - This Guideline specifies the concrete rules for the management and the processing of police information, notably within the scope of international police cooperation. Thus, this Guideline provides rules for managing access to police data, including security issues. These rules also cover loggings and operating instructions for specific applications.
   - The GPI 75 Common Guideline of the Federal Public Service of the Interior (FPSI) and the Federal Public Service of Justice (FPSJ) on the rules of procedure for the police services in the context of indirect access to the personal data they process in the General National Database in the context of the performance of their missions of judicial and administrative police
     - This Guideline provides for precise rules of procedure for the police services in their relation with the CPP concerning the indirect access.
   - The Belgian Act of 8 December 1992 for the Protection of Privacy in relation to the Processing of Personal Data and the Royal Decree of 13 February 2001 implementing it
     - This Act applies the rules of European Directive 95/46/EC to the police sector except for the obligation to inform data subjects about their data being processed. Regarding the rights of access, rectification and deletion in the police sector, the Belgian Privacy Act provides for indirect access.
4. **Number of complaints from data subjects**:
   2013: 26 requests
   2014: 22 requests
   2015: 35 requests
   (see attached tables with details)

5. **Main issues object of complaints**:
   Visa refused
   Excessive checks by police
   Identity issues (alias cases)
   Problems related to passport, plate number, vehicle
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   2013: 26 requests
   2014: 22 requests
   2015: 35 requests
   (see attached tables with details)
   a. Among those, number of requests for deletion that resulted in deletion
   4 deletions (1 correction in progress)
7. **Number of handled cases of cooperation between DPAs:**
   4 requests for cooperation
   a. Among those, number of cases which outcome was data deletion:
   0 deletion
8. **Number of inspection actions performed:**
   2013: Inspection of the Casablanca Consulate
   2014: 5 inspections
   Ministry of Foreign Affairs
   Ministry of Internal Affairs, Department for Aliens Matters
   SIRENE Bureau: check of a sample of the files
   Aliens Office: check of a sample of the files
   Inspection of the London Embassy
   2015: Organizational and technical inspection
9. **Raising awareness activity**: Website information updated in 2015
10. **Link for Schengen information in the DPA website:**
    https://www.privacycommission.be/en/SIS
11. **Any relevant case-law:**
    Not in the period analysed
12. **Any other relevant activity:**
    Schengen Evaluation of Belgium in 2015
    Participation by the Secretariat in 2 SCHEVAL inspections in 2015

3. Bulgaria

1. **Country**: Bulgaria
2. **Name of the DPA:** Commission for Personal Data Protection
3. **Legal provisions implementing SIS II framework (short description):**The national legal framework, related to the processing of personal data by SIS II, includes the following primary legal acts:

- Constitution of the Republic of Bulgaria – Article 32 concerning privacy; Article 5, para. 4 concerning the precedence of international treaties (which have been ratified, promulgated and enacted and thus constitute integral part of the national legislation) over national legislation;
- Ministry of Interior Act (MIA) and the related secondary legislation.
- Law for Protection of Personal Data (LPPD) and the related secondary legislation (Rules of Procedure of the Commission for Personal Data Protection and Its Administration and Ordinance No. 1 dated 30 January 2013 on the minimum level of technical and organizational measures and the admissible type of personal data protection);

Important aspects of personal data protection, related to SIS II, are also regulated by other legal acts, such as the Foreigners in the Republic of Bulgaria Act (prohibiting the entry and stay of third-country nationals), the Asylum and Refugees Act (setting out the principle of non-refoulement), the Extradition and European Arrest Warrant (EAW) Act, Criminal Procedure Code (alerts concerning items which are sought after as evidence), the Code of Criminal Procedure, the Customs Act (alerts to SIS, related to violations of the customs legislation), the Bulgarian ID Documents Act (alerts in accordance with lit. “d” and “e” of Article 38 (2) of Council Decision 2007/533/JHA), the Roads Traffic Act (keeping of registers of vehicles and drivers), the State Agency for National Security Act (discrete surveillance), the Code of Administrative Procedure (judicial control).

The specific rules for the organization and operation of the national system (N.SIS) are set out in Ordinance No. 8121з-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria. In accordance with Article 14 of the Ordinance, data processing at N.SIS is carried out in compliance with the Ministry of Interior Act and the Law for Protection of Personal Data and the subsidiary legislation, related to their application.

4. **Number of complaints from data subjects**: none
5. **Main issues object of complaints**: none

6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: none
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**:

In 2015, the Commission for Personal Data Protection was referred with an alert by a Bulgarian citizen, who has purchased a car from Italy. It was established during the registration that Italy has entered an alert in SIS II, regarding the same vehicle. The car had been bought by its previous owner with a fake cheque. Cheque forgery is considered a crime in Italy. An ad hoc check of the SIRENE Bureau was carried out by a team from the Commission for Personal Data Protection. It was established that the actions performed by the personnel working there were in accordance with Decision 2007/533/JHA and Ordinance No. 8121з-465 of 26 August 2014 on the organisation and functioning of the National Schengen Information System of the Republic of Bulgaria. Furthermore, with regard to the processing of the personal data of the affected person, violation of the provisions of the LPPD was not established.
The Commission for Personal Data establishes informal contacts, in connection to its powers, aiming to expedite the communication between the individual SIRENE Bureaux. In this way, the rights of the affected persons are guaranteed.
A good example is the deletion of personal data of a person, which contributed to the more effective cooperation between the SIRENE Bureaux of Bulgaria and Malta.

    a. Among those, number of cases which outcome was data deletion: 1
8. **Number of inspection actions performed**: CPDP performs checks of the SIRENE Bureau and N.SIS every two years and ad hoc checks on complaints and alerts. Scheduled checks were performed in October 2009, February 2011 and February 2013.

The result of the inspections and the conclusions of the inspection teams were as follows:
- regarding the N.SIS inspection: the necessary technical and organisational measures for personal data protection have been undertaken;
- regarding the inspection of the SIRENE Bureau:

- ✓ the 2009 inspection – there is readiness to apply the personal data protection rules regarding the Schengen-related issues.
- ✓ the 2011 inspection – a binding instruction has been issued and subsequently fulfilled.
- ✓ the 2013 inspection – the provisions of LPPD are complied with while performing the activity (after Bulgaria's accession to the Schengen Area an additional check of the observance of the rules for personal data processing

by SIS II will be performed). The conclusion of the latest check, carried out in 2013, was that the SIRENE Bureau and the International Operative Cooperation Directorate of the Ministry of Interior perform its activity in accordance with the Law for Protection of Personal Data. After Bulgaria's accession to the Schengen Area, an additional check of the compliance with the personal data protection regulations by SIS II will be carried out.

In March 2015, CPDP performed an ad hoc check of the SIRENE Bureau acting on an alert, submitted by a citizen about a breach of rights. The main objectives of the ad hoc check were as follows:

1. Carrying out the cooperation between the Commission for Personal Data Protection and SIRENE Bureau in practice, regarding the checks in cases of complaints and alerts from persons.
2. Clarifying the circumstances, concerning the alert from the person.

The check concluded with the issuance of a Statement of Findings, where the inspection team established that the processing of data by SIS and the subsequent actions of the officers were in accordance with LPPD, Regulation No. 8121з-465 of 26 August 2014 and Decision 2007/533/JHA.

9. **Raising awareness activity**: The Ministry of Interior and the Commission for Personal Data Protection use their web-sites for increasing citizens' awareness, with regard to personal data protection. General information about personal data protection in the Schengen Area, as well as topical information about SIS II, is published (both in Bulgarian and English) in the respective sections of the web-sites of the authorities.

   In addition, all individuals, whose data is processed in the SIS II are recognised
   the right of access to data relating to them stored in the SIS II and the right of correction of inaccurate data or deletion when data have been unlawfully stored. Anyone can exercise these rights by applying to the Commission for Personal Data Protection, using the model letters for requesting access to information and for requesting correction or deletion of the data processed, which could be found on the web-site of the Commission for Personal Data Protection.
   Brochures and a leaflet, regarding the Schengen Area, SIS II and the personal data in SIS II will be published on the web-site of the Commission for Personal Data Protection.

10. **Link for Schengen information in the DPA website**: The dedicated section from the web-site of the Commission for Personal Data Protection is currently being updated. Links to the official web-sites of the Ministry of

Interior, the Ministry of Foreign Affairs and Directorate General Migration and Home Affairs of the European Commission will be established.

11. **Any relevant case-law**: none
12. **Any other relevant activity**: In 2015 Bulgaria carried out a self-evaluation with regard to the Schengen acquis. It was under the aegis of the Ministry of Interior, with the participation of the Commission for Personal Data Protection and the Ministry of Foreign Affairs.

4. Republic of Croatia

1. **Country**: Republic of Croatia
2. **Name of the DPA**: Personal Data Protection Agency
3. **Legal provisions implementing SIS II framework (short description)**: Yes, Personal Data Protection Act („Official Gazette" number: 103/03, /06, 41/08 and 130/11; 106/12 - consolidated text;) represents the basis which regulates the personal data protection of natural persons, and the supervision of collection, processing and usage of personal data in the Republic of Croatia. Provisions of this Act shall apply to the personal data processing conducted by state bodies, local and regional self-government units, as well as by legal and natural persons, representation offices and branches of foreign legal persons, and representatives of foreign legal and natural persons processing personal data (Article 3. Paragraph 1.) Therefore, this regulation also applies to the dana processing system SIS II. Personal Data Protection Act is a general act which applies on processing of personal data in Schengen Information System II. The personal data filing systems which are kept by the Ministry of the Interior, as data controller, are regulated with Police Duties and Powers Act as a special act and with Personal Data Protection Act as a general act.
4. **Number of complaints from data subjects**: 0
5. **Main issues object of complaints**: -
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: The Agency has received a total of 3 requests for access to personal data
    a. Among those, number of requests for deletion that resulted in deletion: 0
7. **Number of handled cases of cooperation between DPAs**: 0
    a. Among those, number of cases which outcome was data deletion: 0
8. **Number of inspection actions performed**: 0

9. **Raising awareness activity**: The Agency is preparing a Guide for exercising the right of access to the SIS II in order to inform the public about their rights and the ways to exercise them.
10. **Link for Schengen information in the DPA website**: The preparation of the Guide on exercising the right to access to the SIS II is in progress.
11. **Any relevant case-law**: No
12. **Any other relevant activity**: No

Remark:

In addition to the said, the Agency wishes to point out that the Republic of Croatia is in the process of Schengen evaluation regarding the necessary requirements for the establishment of the Schengen Information System, and therefore we didn't have any direct experience and the practical actions in the context of the mentioned system.

5. Cyprus

1. **Country**: CYPRUS
2. **Name of the DPA**: COMMISSIONER FOR PERSONAL DATA PROTECTION
3. **Legal provisions implementing SIS II framework (short description)**: A draft bill is in the pipeline for the better implementation of Decisions 2007/533/JHA and 2007/171/JHA and Regulations 1987/2006 and 1986/2007.
4. **Number of complaints from data subjects**: N/A
5. **Main issues object of complaints**: N/A
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: The rights of access, correction and deletion will be exercised directly to the Police.
    a. Among those, number of requests for deletion that resulted in deletion: N/A
7. **Number of handled cases of cooperation between DPAs**: N/A
    a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: N/A
9. **Raising awareness activity**: N/A
10. **Link for Schengen information in the DPA website**: N/A
11. **Any relevant case-law**: N/A
12. **Any other relevant activity**: N/A

6. Czech Republic

1. **Country**: The Czech Republic
2. **Name of the DPA**: The Office for Personal Data Protection
3. **Legal provisions implementing SIS II framework (short description)**: Act Nr. 101/2000 Coll., on the Protection of Personal Data (this Act regulates the rights and obligation in processing of personal data and entrusts the Office for Personal Data Protection with the competence of central administrative authority in the area of personal data protection.
4. **Number of complaints from data subjects**: 181 complaints sent to the Police of the Czech Republic acting as a data controller
5. **Main issues object of complaints**: exercise of the right to have access to the information being processed, right for deletion of unlawfully stored data
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: 11
    1. Among those, number of requests for deletion that resulted in deletion: DPA does not have access to this kind of information; it is exclusively reserved to the Police of the Czech Republic.
7. **Number of handled cases of cooperation between DPAs**: 0
    2. Among those, number of cases which outcome was data deletion: information belongs to the Police of the Czech Republic, and is not shared with the Office for Personal Data Protection
8. **Number of inspection actions performed**: 0
9. **Raising awareness activity**: DPA web site
10. **Link for Schengen information in the DPA website**: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1366&archiv=0&p1=1221
11. **Any relevant case-law**: no
12. **Any other relevant activity**: three national experts were nominated to evaluate the level of data protection in accordance with the Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen in Belgium, Germany and Lichtenstein.

7. Denmark

1. **Country**: Denmark
2. **Name of the DPA**: Datatilsynet
3. **Legal provisions implementing SIS II framework (short description):**
   The rules implementing the SIS II framework in Denmark are Act no. 418 of 10 June 1997, Act no. 227 of 2 April 2003, Act no. 448 of 9 June 2004, and Act no. 521 of 6 June 2007.
   The act from 1997 implements the Schengen Convention and the acts from 2003, 2004, and 2007 amend the Danish "Schengen Convention act" in accordance with the Schengen Decision and Schengen II Regulation.
4. **Number of complaints from data subjects**:
   1 complaint was handled by the Danish DPA.

   The DPA forwards complaints to the Danish Nation Police as the first instance. If the data subject is not happy about the National Police's decision the subject can file a complaint to the DPA.
5. **Main issues object of complaints**: Access.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   Approximately 27 requests to the Danish DPA (requests are forwarded to the Danish National Police as the first instance, see the above).
   a. Among those, number of requests for deletion that resulted in deletion
      0 (If a forwarding, cf. no. 4, of a request to the Danish National Police has resulted in deletion the Danish DPA won't necessary be noted).
7. **Number of handled cases of cooperation between DPAs**:
   7 (some of the cases are started before 2013 but ended in the period of 2013-2015)
   a. Among those, number of cases which outcome was data deletion:1
8. **Number of inspection actions performed**:
   2014: Schengen inspection at the Danish embassy in London.
   2015: Examination of the case concerning unauthorized access to personal data in SIS II ("The hacker case").
9. **Raising awareness activity**:
   The Danish DPA has planned to inform the Danish Ministry of Justice, the Danish National Police, and the Danish Immigration Service about, inter alia, the Guide for the exercise of access to SIS II.
   Due to a heavy workload this hasn't been done in 2015 but the Danish DPA plans to do it in 20156
10. **Link for Schengen information in the DPA website:**

https://www.datatilsynet.dk/internationalt/schengen-samarbejdet/ (Danish)
https://www.datatilsynet.dk/english/your-rights-in-relation-to-the-schengen-information-system/ (English)

11. **Any relevant case-law:**
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Schengen/Afgoerelse_af_24._september_2001.pdf (Decision from the Danish DPA regarding access)
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/On-line_hoeringssvar_-_Nyhed_16_6-03/Datatilsynets_udtalelse_hackcase.pdf
(Decision from the Danish DPA regarding unauthorized access to personal data – "the hacker case")
12. **Any other relevant activity: N/A**

8. Republic of Estonia

1. **Country:** Republic of Estonia
2. **Name of the DPA**: Estonian Data Protection Inspectorate
3. **Legal provisions implementing SIS II framework (short description)**:
National register of SIS is regulated in Police and Border Guard Act12 §§ 20-25 and by a statute13 governing its maintenance.
The data subject has to send an application to the Estonian Police and Border Guard Board (PBGB, the chief processor) or to the Estonian Data Protection Inspectorate (DPI) in order to request access, correct, delete or obtain information.
The application must entail at least the applicant's name, date of birth, citizenship, signature, copy of an identification document, the nature and circumstances of the application. Estonian citizens and e-residents can provide a digital signature to their application. In other cases the data subject has to provide a handwritten signature. There are no other distinctions regarding a data subject's origin – whether he/she is from Estonia, from another Schengen member state or from a third country. Person receives an answer to his/her application within 30 days. The processes in the PBGB and DPI are free of charge. If the data subject is not satisfied with the PBGB's answers, he/she can file a complaint to the DPI or to the court. If the data subject is not satisfied with the outcome of the procedure in the DPI, he/she can turn to the court. If the data subject wishes to seek compensation for the

[12] Police and Border Guard Act https://www.riigiteataja.ee/akt/118042013027 (in English).
[13] Statute on the maintenance of the national register of the Schengen Information system: https://www.riigiteataja.ee/akt/118042013027 [in Estonian).

alert, then he/she has to lodge a complaint to court. Court proceedings are not free.

4. **Number of complaints from data subjects**: No complaints. We note that primarily we dealt with cases where a person wished to access their data, but data subjects did not lodge a complaint if they received what was in the SIS II about them. If in fact there was outdated data in the SIS II, then the data was updated while processing the access request.
5. **Main issues object of complaints**: N/A
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   2013 – 6 cases; 2014 – 6 cases; 2015 – 10 cases.
   a. Among those, number of requests for deletion that resulted in deletion: In 2013 one case, in 2014 one case, and in 2015 zero cases.
7. **Number of handled cases of cooperation between DPAs**: None.
   a. Among those, number of cases which outcome was data deletion: N/A
8. **Number of inspection actions performed:**
   We did 2 on the spot inspections, where we wished to know:
   - how the national SIRENE bureau implements the requirements for data processing (entering alerts) in SIS II;
   - how data processing rules are complied in a prefecture level (alerts are forwarded from a prefectural authority to national SIRENE bureau for entering them to SIS II).
9. **Raising awareness activity:**
   Estonian DPA is concentrated on raising awareness by digital means. In three languages we keep relevant information and links on our website, on national police website and Ministry of Foreign Affairs' website. We also provide information and possible appeal to DPA on paper at the border points in relevant languages.
10. **Link for Schengen information in the DPA website:**
    a. http://www.aki.ee/et/rahvusvaheline-koostoo/schengen (in Estonian);
    b. http://www.aki.ee/en/international-cooperation/schengen (in English);
    c. http://www.aki.ee/ru/shengen (in Russian).
11. **Any relevant case-law:**
    a. currently no case law – data subjects generally wish to have access on what personal data about them is entered in SIS – therefore they turn for answers to DPI or PBGB
12. **Any other relevant activity: -**

9. Finland

1. **Country**: Finland
2. **Name of the DPA**: Office of the Data Protection Ombudsman
3. **Legal provisions implementing SIS II framework (short description)**:
   Police Data Protection Act, General Act on the police data protection and the processing of personal data by the police.
4. **Number of complaints from data subjects:**
   No complaints. Numerous inquiries how to check your information in SIS etc.
5. **Main issues object of complaints**: --
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   a. Among those, number of requests for deletion that resulted in deletion

   None

   Direct access, rights are not exercised via DPA
7. **Number of handled cases of cooperation between DPAs**:
   a. Among those, number of cases which outcome was data deletion:

   None
8. **Number of inspection actions performed**:
   No inspection specially focused on SIS. Several activities focused at police data processing, which are also related to SIS. Planning of a comprehensive SIS inspection during 2016.
9. **Raising awareness activity**:
   Web page of the police:
   https://www.poliisi.fi/services/checking_personal_data
10. **Link for Schengen information in the DPA website**:
    http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/kansainvalinenyhteistyo/valvontaelimet_0.html
11. **Any relevant case-law:**
12. **Any other relevant activity:**

10. France

1. **Country**: FRANCE
2. **Name of the DPA**: Commission nationale de l'informatique et des libertés (CNIL)
3. **Legal provisions implementing SIS II framework (short description):**

The Schengen information system II is regulated by two legal instruments at the European level: Decision 2007 / 533 / JAI of the Council of June 12th, 2007 on the establishment, the functioning and the use of the information system second generation Schengen (SIS II), in particular its chapter XII, and Regulation n° 1987/2006 of the European Parliament and the Council(Advise) of December 20th, 2006 on the establishment, the functioning and the use of the information system second generation Schengen (SIS II), in particular chapter VI.

At national level, the French data protection act (known as loi " Informatique et Libertés ") of January 6th, 1978 regulates data processing carried out on behalf of the State, for purposes of public safety, defense or public security or which purpose is the prevention, the investigation, the detection or the prosecution of the criminal offenses or the execution of the criminal penalties or the security measures.

Following the French data protection act, the national part of the Schengen information system (N-SIS,) has to be regulated by a specific decree. The N-SIS was regulated by the decree n° 95-577 of May 6th, 1995 relating to the national Schengen Information System (hereinafter N-SIS) (formally adopted upon prior opinion of the CNIL.

This decree has been repealed and its regulatory measures relative to N-SIS were integrated into the internal security code.

4. **Number of complaints from data subjects**: **0**
5. **Main issues object of complaints**: **n/a**
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:

	2013	2014	2015
Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)	260	261	234
Number of requests that resulted in deletion	12	8	9

7. **Number of handled cases of cooperation between DPAs**:

	2013	2014	2015
Number of handled cases of cooperation between DPAs	35	34	37

The response times of these foreign supervisory authorities improved since 2012. CNIL rarely receives requests from other supervisory authorities.

a. Among those, number of cases which outcome was data deletion: **n/a**

8. **Number of inspection actions performed:**
   EU large scale IT systems used in the framework of police cooperation are on the CNIL's annual inspection program for 2015/2016. In this context, several inspections have been carried out. Their exact number cannot be disclosed are the procedure is not yet finalized and remains confidential at this stage.
9. **Raising awareness activity:**
   In the context of the upcoming Schengen evaluation, the CNIL is rethinking the content of its website relating to SIS II. New information pages are under drafting which will bring a more pedagogic approach. In the meantime, the CNIL has published the guide on access of data subjects to SIS II on its website. Numerous contacts were taken with the SIS II competent public authorities which lead the way to an enhanced cooperation.
10. **Link for Schengen information in the DPA website:** https://www.cnil.fr/fr/sis-systeme-dinformation-schengen
11. **Any relevant case-law:** N/A
12. **Any other relevant activity**: N/A

11. Germany

1. **Country**: Germany
2. **Name of the DPA**: Federal Commissioner for Data Protection and Freedom of Information
3. **Legal provisions implementing SIS II framework (short description)**:
   - Act on the Schengen Information System II (Gesetz zum Schengener Informationssystem der zweiten Generation - SIS-II-Gesetz)
     Affected regulations:
     - Criminal Investigation Act (Bundeskriminalamtgesetz– BKAG)
     - Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (Bundesverfassungsschutzgesetz - BVerfSchG)

- The German Code of Criminal Procedure (Strafprozeßordnung – StPO)
- Act of 15 July 1993 on the Schengen Agreement of 19 June 1990 on the Gradual Abolition of Checks at the Common Borders (Gesetz zu dem Schengener Übereinkommen vom 19. Juni 1990 betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen)
- Act supplementing the Counter Terrorism Act (Terrorismusbekämpfungsergänzungsgesetz)

4. **Number of complaints from data subjects**: 205
5. **Main issues object of complaints**: requests for access
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**
   - requests for access: 107
   - requests for correction: 0
   - requests for deletion: 98

   a. Among those, number of requests for deletion that resulted in deletion
      - 14
7. **Number of handled cases of cooperation between DPAs**:
   - 23

   a. Among those, number of cases which outcome was data deletion:
      - 10
8. **Number of inspection actions performed**:
   - 1
9. **Raising awareness activity:**
   - Leafleat
   - Online: Information on Website + A GUIDE FOR EXERCISING THE RIGHT OF ACCESS
10. **Link for Schengen information in the DPA website:**
    http://www.bfdi.bund.de/DE/Europa_International/Europa/Justizielle_und_polizeiliche_Zusammenarbeit/Polizeiliche_Zusammenarbeit/SchengenerInformationssystem-Allgemeines.html;jsessionid=335E5EAEEEB7FCBFCB3669058E097F65.1_cid329?cms_templateQueryString=schengen+information+system&cms_sortOrder=score+desc
11. **Any relevant case-law**: -
12. **Any other relevant activity**: -

12. Greece

1. **Country**: Hellas.
2. **Name of the DPA**: Hellenic Data Protection Authority.
3. **Legal provisions implementing SIS II framework (short description):**
   No national legal provisions implementing SIS II were introduced.
4. **Number of complaints from data subjects**:
   2013: 20
   2014: 24
   2015: 25
5. **Main issues object of complaints:**
   Request for deletion.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**
   a. Among those, number of requests for deletion that resulted in deletion

   N/a (the rights of access, correction and deletion are exercised directly to the data controller – Hellenic Police and in particular to the SIRENE Bureau)
7. **Number of handled cases of cooperation between DPAs**:
   2013: 3 cases
   2014: 5 cases
   2015: 5 cases
   a. Among those, number of cases which outcome was data deletion: 1
8. **Number of inspection actions performed**:
   One on-site inspection.
9. **Raising awareness activity:**
   Information provided by the HDPA' s website (Guide for exercising the right of access, etc) and the quarterly issued newsletter which is published in that website and cites the more important Decisions (amongst which Schengen related Decisions on request for deletion can be found) delivered by the Board of the HDPA.
10. **Link for Schengen information in the DPA website:**
    http://www.dpa.gr/portal/page?_pageid=33,126607&_dad=portal&_schema=PORTAL (in Greek)
    http://www.dpa.gr/portal/page?_pageid=33,67046&_dad=portal&_schema=PORTAL (in English)
11. **Any relevant case-law:**
    None in this time frame
12. **Any other relevant activity:**
    None

13. Hungary

1. **Country:** Hungary
2. **Name of the DPA:**
   Hungarian National Authority for Data Protection and Freedom of Information
3. **Legal provisions implementing SIS II framework (short description):**
   Provisions on the use of SIS II are implemented in Act CLXXXI of 2012 on information exchange within the framework of the Second Generation Schengen Information System. The provisions of the act are normative in Hungary regarding data processing issues in the SIS II.
4. **Number of complaints from data subjects**: 35
5. **Main issues object of complaints**:
   Information or deletion requests from the SIS II
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: 35
   a. Among those, number of requests for deletion that resulted in deletion: 0
7. **Number of handled cases of cooperation between DPAs**: 2
   a. Among those, number of cases which outcome was data deletion: 0
8. **Number of inspection actions performed**: 6
9. **Raising awareness activity:** -
10. **Link for Schengen information in the DPA website:**
    In Hungarian: http://www.naih.hu/schengeni-informacios-rendszer.html
    In English: http://www.naih.hu/schengen-information-system.html
11. **Any relevant case-law: -**
12. **Any other relevant activity:** On conferences organized by the Hungarian DPA, short informative prospectuses about data subject rights are often circulated among participant.

14. Iceland

1. **Country**: Iceland.
2. **Name of the DPA**: The Data Protection Authority (DPA).
3. **Legal provisions implementing SIS II framework (short description):** Act No. 16/2000 on the Schengen Information System in Iceland. Regulation No. 112/2001 on the Schengen Information System in Iceland.
4. **Number of complaints from data subjects**: No complaints were received.

5. **Main issues object of complaints**: N/A.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA**): The DPA received one access request in 2013 and one in 2015. In both instances, the individual in question was redirected to the National Commissioner of the Icelandic Police, which is responsible for handling such requests.
    a. Among those, number of requests for deletion that resulted in deletion: In the aforementioned instances, deletion was not requested.
7. **Number of handled cases of cooperation between DPAs**: N/A.
    a. Among those, number of cases which outcome was data deletion: N/A.
8. **Number of inspection actions performed:** No inspections specifically aimed at SIS II were performed. However, information on the processing was gathered in line with decisions taken by the SIS II SCG. Furthermore, the International Unit of the National Commissioner of the Icelandic Police, which is responsible for SIS II processing, underwent an inspection by the DPA regarding advance deletion of Eurodac data.
9. **Raising awareness activity**: Information has been published on the website of the DPA, cf. the answer to Point 10.
10. **Link for Schengen information in the DPA website**: Information on the Schengen Information System can be found here: http://www.personuvernd.is/information-in-english/
11. **Any relevant case-law:** No relevant case law.
12. **Any other relevant activity**: N/A.

15. Italy

1. **Country**: ITALY
2. **Name of the DPA**: Garante per la protezione dei dati personali
3. **Legal provisions implementing SIS II framework (short description):** No changes in legislation
4. **Number of complaints from data subjects:** NO complaints were received by the DPA during the referred period. The DPAs received access requests sent sent as well to the competent national authority.
5. **Main issues object of complaints**: =. As for the above mentioned requests they were maily dealing with Article 24 of the Regulation
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: =

   a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: 2013:15; 2014:21; 2015: 13
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: No in situ inspections performed, but rather checks on specific issues + activities linked to the follow up of prescriptive measures adopted by the Garante and check the state of the implementation.
9. **Raising awareness activity:** updating of the Garante website including reference and link to the guide on the exercise of the right of access and link to MoI website.
10. **Link for Schengen information in the DPA website**: http://www.garanteprivacy.it/web/guest/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/schengen
11. **Any relevant case-law**:NONE
12. **Any other relevant activity**: Activities performed for the Schengen evaluation of Italy in the field of data protection which took place in March 2016.

16. Latvia

1. **Country:** Latvia
2. **Name of the DPA**: Data State Inspectorate
3. **Legal provisions implementing SIS II framework (short description):**
   - Law on Operation of the Shengen Information System
   - Regulations of the Cabinet of Ministers No. 639 of 18 September 2007 Procedures for the Entering, Correction and Deletion of Alerts in the Schengen Information System, as well as Ensuring Accessibility of Supplementary Information between the SIRENE Latvia Bureau and Procedures for the Exchange of Supplementary Information of Institutions and Authorities
   - Regulations of the Cabinet of Ministers No. 622 of 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System
4. **Number of complaints from data subjects**: In 2015 - 1

5. **Main issues object of complaints:** Personal data procession (personal data correction)
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**:
    a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: 1
9. **Raising awareness activity**:
10. **Link for Schengen information in the DPA website**:
    http://www.dvi.gov.lv/lv/saites/ (Latvian version)
    Section: Informācija par Šengenas Informācijas sistēmu SIS II
    Section: Šengenas informācijas sistēma (Latvijas valsts daļa)
    http://www.dvi.gov.lv/en/personal-data-protection-2/international-cooperation/ (English version)
11. **Any relevant case-law**: N/A
12. **Any other relevant activity**: In general the number of complaints received in DSI is not increasing significantly

17. Liechtenstein

1. **Country**: Liechtenstein
2. **Name of the DPA**: Data Protection Office
3. **Legal provisions implementing SIS II framework (short description):**
    The Regulation (EC) No 1987/2006 (SIS II Regulation) and the Council Decision 2007/533/JHA (SIS II Decision) have been implemented in Liechtenstein in a separate Ordinance, the N-SIS-Ordinance. It is based on the Police Act and the Foreigner Act. The Ordinance regulates especially the following:
    a) The organisation and the tasks of the SIRENE bureau as well as its case handling system (SIRA);
    b) The national part of the Schengen Information System (N-SIS);
    c) The access rights and jurisdictions of the authorities with regard to the N-SIS;
    d) The exchange of additional information through the SIRENE bureau;
    e) The processes, prerequisites, measures and flagging of the personal and property alerts within N-SIS;

f) The handling and retention period of the data;

g) The rights of the persons involved;

h) The data security, data protection consulting as well as the supervision of the processing of data. (Art. 1 N-SIS-Ordinance)

4. **Number of complaints from data subjects**:
   0
5. **Main issues object of complaints**:
   n/a
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   requests are exercised directly at the National Police.
   a. Among those, number of requests for deletion that resulted in deletion – n/a

7. **Number of handled cases of cooperation between DPAs**: 0
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed:**
   1 audit regarding the SIS-query-client at the Migration and Passport Office.
9. **Raising awareness activity:**
   Information regarding SIS and Schengen/Dublin is available on the data protection office website. The website of the National Police has been linked to the one of the data protection office in Liechtenstein.
   In connection with the enrolment of SIS II an information campaign was launched. Additional information was published on the websites, a newsletter was sent and an article informing about the migration and the newly established SIS II was published in both newspapers of Liechtenstein.
10. **Link for Schengen information in the DPA website**:
    http://www.llv.li/#/117356/schengendublin (in English).
11. **Any relevant case-law:** n/a
12. **Any other relevant activity**: n/a

18. Lithuania

1. **Country:** LITHUANIA
2. **Name of the DPA**: The State Data Protection Inspectorate
3. **Legal provisions implementing SIS II framework (short description):**
   Data processing in second generation Schengen Information System SIS II comply with the requirement of the 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, Council Decision 2007/533/JHA of 12 June 2007 in accordance with the act on the second generation Schengen Information System (SIS II), the law on legal protection of personal data of the Republic of Lithuania, Lithuanian national Schengen Information System regulations, approved by the Order No 1V-324 of 17 September 2007 by the Minister of the Interior, the Safety Regulations of Lithuanian national Schengen Information System approved by the Order No 1V-325 of 17 September 2007 by the Minister of the Interior. Alerts which shall be submitted to the SIS II are generated in national registers and shall comply with the requirements of data security approved by relevant institutions.

4. **Number of complaints from data subjects**: No
5. **Main issues object of complaints**: No
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: 12 requests
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: No
    a. Among those, number of cases which outcome was data deletion: No
8. **Number of inspection actions performed**: No
9. **Raising awareness activity:**
   The State Data Protection Inspectorate updated information (SIS II new opportunities, the data subjects' rights of access, rectification, modification and unauthorized use of personal data, the list of competent institutions which are authorized to use data stored in the SIS II) published on its website immediately after 9th of April 2013 when the SIS II has been launched. All relevant information about SIS II has been submitted to the competent institutions (ministry of the Interior of the Republic of Lithuania, Migration Department under the Ministry of the Interior of the Republic of Lithuania, Information technology and communications Department under the Ministry of the Interior of the Republic of Lithuania) for the publication, this information on their websites by the state.
   Data Protection Inspectorate. Information regarding the exercise of data subjects' rights in second generation Schengen Information System is continuously updated.
10. Link for Schengen information in the DPA website:
    http://www.ada.lt/go.php/lit/IMG/361/7 (in Lithuanian)
    http://www.ada.lt/index.php?action=page&lng=en&id=273 (in English)
11. **Any relevant case-law**: No
12. **Any other relevant activity:**
    In 2015 the SIRENE bureau has been checked by the State Data Protection Inspectorate for access to the national Visa Information System. In practice, the need to check visas in national Visa Information System by SIRENE

Bureau arises upon request from Member States attesting that a visa has been legally issued, or has been falsified in order to determine if a person is legally within the Schengen Area.
Information is exchanged via SIRENE channel exclusively in investigating cases, where there is an alert on refusal of entry or stay in the Schengen area on third country national in accordance with Article 24 of the 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) and this person submitted a Schengen visa issued by Lithuania. In such cases, first it will be checked whether a visa submitted is actually valid.

19. Luxembourg

1. **Country**: LUXEMBOURG
2. **Name of the DPAs**: Supervisory Authority "Article 17" which has exclusive competence to supervise processing of personal data carried out by the Police, Intelligence services, Customs authority and Army.
   The "ordinary » DPA is called "Commission Nationale pour la Protection des Données (CNPD)"
3. **Legal provisions implementing SIS II framework (short description):** There is no specific national legislation implementing SIS II framework. Council Decision 2007/533/JHA, Regulation 1987/2006, Regulation 1986/2006 and the national data protection Law of 2 August 2002 are applicable.
4. **Number of complaints from data subjects**: None
5. **Main issues object of complaints**: n/a
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:
   2013: 4
   2014: 2
   2015: 3
   a. Among those, number of requests for deletion that resulted in deletion : None
7. **Number of handled cases of cooperation between DPAs:** None
   a. Among those, number of cases which outcome was data deletion: n/a
8. **Number of inspection actions performed**: 1
9. **Raising awareness activity**: Publication on the DPA's website of the "Guide for exercising the right of access" compiled by the SIS II Supervision Coordination Group and publication of model letters for exercising the right of access
10. **Link for Schengen information in the DPA website:**

http://www.cnpd.public.lu/en/commission-nationale/autorite-specifique/SIS-II-SCG/index.html

11. **Any relevant case-law:** None
12. **Any other relevant activity:** During the second half of 2015, the Luxembourg DPA prepared the Schengen Evaluation which took place in January 2016

20. Malta

1. **Country:** Malta
2. **Name of the DPA:**
   Information and Data Protection Commissioner
3. **Legal provisions implementing SIS II framework (short description):**
   The processing of personal data in the law enforcement sector is primarily regulated by Subsidiary Legislation 440.05 extending the applicability of the Data Protection Act (Chapter 440 of the Laws of Malta) to the Police Sector. These regulations are based on the data protection principles contained in Recommendation 87(15) of the Council of Europe. Additionally in this area, Subsidiary Legislation 440.06 specifically regulates the exchanges of personal data for Police and Judicial cooperation in criminal matters, thus implementing the Council Framework Decision 2008/977 JHA. Exemptions may be applicable when exercising the rights of data subjects, in particular, the provision of information, right of access, rectification, blocking or erasure of personal data. These exemptions may be applied when a law specifically provides for the provision of information as a necessary measure for the prevention, investigation, detection and prosecution of criminal offences (Article 23(d) of Chapter 440 of the Laws of Malta), or where a restriction or refusal of such rights is justified for the purpose of the suppression of criminal offences, or necessary for the protection of the individual or the rights and freedoms of others (Reg 13, SL440.05), or to avoid obstructing official or legal inquiries, investigations or procedure (Reg 17, SL440.06).
   In addition, specific regulations established under a Police GHQ Circular No: 115/07 titled 'Schengen Information System Regulations' recognize the Data Protection Officer of the Malta Police Force as being responsible for the receipt, processing and replies of Data Subject Access Requests, and lists the authorities which may have access to alerts of the SIS II.
4. **Number of complaints from data subjects:**
   No complaints were received during the period under review.
5. **Main issues object of complaints**: N/A
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**

In Malta the rights of access, correction and deletion are directly exercisable with the data controller, in this case the Police. This notwithstanding, during the period under review, our DPA received 20 requests for access and deletion in relation to SIS alerts. In similar cases, the data subjects are referred to the guidelines available on our website, and are advised to redirect their request to the Data Protection Officer of the Police, being the responsible body to handle such requests, as data controller for SIS II.

a. Among those, number of requests for deletion that resulted in deletion

Given that the requests are made with the Police, this Office does not have similar statistics.

7. **Number of handled cases of cooperation between DPAs:**

   There were no specific cases involving cooperation with other DPAs during such period.

   a. Among those, number of cases which outcome was data deletion:

8. **Number of inspection actions performed:**

   No onsite inspections were performed during the period under review. However, in accordance with the obligation to carry out an audit every four years, the DPA is planning to perform a number of inspections in 2016. These inspections will not only focus on the specific processing in the NS-SIS II but will also consider the procedures in place and the data processes carried out by the different stakeholders involved in SIS II related activities.

9. **Raising awareness activity:**

   The DPA has a specific page on its website dealing with Schengen information. This page provides information on the Schengen Acquis, the SIS, the relevant legal basis, the type of personal data being processed in SIS, and also information on how data subjects may exercise their rights.

   The DPA is also active in encouraging the dissemination of information on SIS and particularly data subjects' rights, especially by the relevant stakeholders involved in the Schengen and Visa procedures (e.g. information on the websites of the relevant Ministries, information leaflets at the Consular posts).

10. **Link for Schengen information in the DPA website:**

    http://idpc.gov.mt/en/Pages/dp/eu/schengen.aspx

11. **Any relevant case-law:**

12. **Any other relevant activity:**

    As from December 2015, our DPA started to coordinate a working group on a national level, with the objective of discussing data protection issues relating to the Schengen and Visa procedures, on a regular basis. The working group consists of representatives from all the relevant stakeholders involved in the Schengen and Visa procedure, such as the Police (NS-SIS, SIRENE and Immigration), the Ministry for Foreign Affairs, the Ministry for Home Affairs,

the Ministry for Social Dialogue and Civil Liberties, the Visa Authorities, the Citizenship Unit, the Refugee Commissioner, and the Identity Agency. The aim of these discussions is to ensure that all stakeholders comply with the applicable data protection legal framework the whole procedure.

21. Norway

1. **Country**: Norway
2. **Name of the DPA**: Datatilsynet/The Norwegian Data Protection Authority
3. **Legal provisions implementing SIS II framework (short description):** The Act relating to the Schengen Information System of 16 July 1999 no. 66, as amended by the Act of 27 June 2008 (entry into force on 9 April 2013)
4. **Number of complaints from data subjects:**
5. **Main issues object of complaints:** N/A
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: 16
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs:** 0
    a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed:** 1
9. **Raising awareness activity:** Information on DPA web site
10. **Link for Schengen information in the DPA website:** https://www.datatilsynet.no/English/The-Schengen-Information-System-SIS/
11. **Any relevant case-law:** N/A
12. **Any other relevant activity:** N/A

22. The Netherlands

1. **Country**: The Netherlands
2. **Name of the DPA**: Autoriteit Persoonsgegevens
3. **Legal provisions implementing SIS II framework (short description):** With respect to processing of SIS II data for law enforcement purposes – as meant in the SIS II Decision – the Police Data Act (Wet politiegegevens) and the Police Data Decree (Besluit politiegegevens) are applicable. No other specific rules or exceptions are foreseen for this category of data. With respect to processing of SIS II data for migration purposes – as meant in the SIS II Regulation – the Data Protection Act (DP Act, Wet bescherming

persoonsgegevens) is applicable. No other specific rules or exceptions are foreseen in this regard.

4. **Number of complaints from data subjects**: 0
5. **Main issues object of complaints**: 0
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**:

   Number of requests for access
   Below, the numbers of request for access regarding SIS, as they were handled by the Netherlands National Police. In the Netherlands those requests are received directly by the Central Unit, as this Unit is appointed as the sole body to handle those requests.
   Only very occasionally the Data Protection Authority receives a request, in which case the DPA forwards this request to the Central Unit, where it will be dealt with.
   Between brackets the number of requests that were received by the National Police via the DPA.

2013	2014	2015
316 (8)	314 (5)	305 (4)

   a. Among those, number of requests for deletion that resulted in deletion

   Number of requests for deletion that resulted in deletion

   Practically all cases where alerts were deleted, concerned the alien alerts. In those cases, the National Police, after having handled the case firstly as a request for access, forwards the request (for deletion) to the Immigration and Naturalization Service, where a decision can be made whether or not the alert will be deleted. Only once in a while it is reported back to the National Police that an alert was deleted, but in most cases the National Police remains unaware of the result.
   The number of cases in which the National Police is informed about the deletion will be given here, but it can be assumed that the numbers will be higher than the figures mentioned here.

2013	2014	2015
8	8	9

7. **Number of handled cases of cooperation between DPAs**: five
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: four
9. **Raising awareness activity**: The website of the DPA (www.autoriteitpersoonsgegevens.nl) has dedicated parts explaining the

functioning of the SIS II. The right of access, rectification, deletion and blocking of personal data. The website provides this information in Dutch and English.

The DPA publishes its annual report on its website. The summary of the annual reports are also available in English on the DPA website. The DPA provides a telephone helpdesk service available also in English that gives quick answers to data protection questions, available from Monday to Friday from 09:30-12:30.

10. **Link for Schengen information in the DPA website**: yes
11. **Any relevant case-law**:
12. **Any other relevant activity:**

Schengen Evaluation of The Netherlands in 2015

23. Poland

1. **Country**: Poland
2. **Name of the DPA:** Inspector General for the Protection of Personal Data (Generalny Inspektor Ochrony Danych Osobowych)
3. **Legal provisions implementing SIS II framework (short description):** Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System sets out the rules and implementing measures for the participation of the Republic of Poland, including public authorities' obligations and rights which concern making entries and access to data in the SIS and VIS via the National Information System.
4. **Number of complaints from data subjects:** 31
5. **Main issues object of complaints**: deletion of data, legality of introducing data to the SIS II, outdated personal data introduced to the SIS II.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):** Right of access in Poland is exercised directly.
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: 2
    a. Among those, number of cases which outcome was data deletion: 1
8. **Number of inspection actions performed**: 39
9. **Raising awareness activity**: Polish DPA performed series of trainings on personal data protection for persons who have access to the SIS, which are additional to the obligatory trainings performed by responsible authorities, which are undertaken in accordance with the Regulation on the methods of

conducting trainings on security and data protection used by National Information System and on qualifications of persons authorised to carry out those trainings.

Polish DPA obliged also competent authorities which have access to SIS II to comply with all the conclusions from questionnaires, reports, and other activities conducted by SIS II SCG. In addition, the Police Commander in Chief (controller) and the DPA published on their websites SIS II A Guide for Exercising the Right of Access.

10. **Link for Schengen information in the DPA website:**
    http://www.giodo.gov.pl/264/j/pl/
11. **Any relevant case-law**: in 2013 -2015 two cases concerning SIS II had been brought to the courts. Both ended in dismissal of the complainants' claims and maintenance of the decision of the Polish DPA: judgment of the Voivod Administrative Court of Warsaw, delivered on 7 May 2014 WSA (ref. nr II SA/Wa 375/14, available online only in Polish:
    http://www.orzeczenia-nsa.pl/wyrok/ii-sa-wa-375-14/sprawy_zwiazane_z_ochrona_danych_osobowych/e25538.html
    and judgement of the Supreme Administrative Court, delivered on 2 December 2015 (ref. nr I OSK 2508/14, available online only in Polish:
    http://www.orzeczenia-nsa.pl/wyrok/i-osk-2508-14/sprawy_zwiazane_z_ochrona_danych_osobowych/229c257.html
12. **Any other relevant activity:** Nothing to report

24. Portugal

1. **Country:** PORTUGAL
2. **Name of the DPA**: Comissão Nacional de Protecção de Dados (CNPD)
3. **Legal provisions implementing SIS II framework (short description):**
   The Data Protection Act (Law 67/98, of 26 October) is applicable to the SIS data processing and covers all competent authorities with access to the SIS. There is also Law 2/94 establishing the control and verification mechanisms for the SIS, which is still applicable to the SIS II legal framework with the necessary adjustments. This law sets the DPA as the national control authority entrusted with the supervision of the national part of the SIS; it provides for an indirect right of access, rectification and deletion via the DPA and it lays down (shorter) deadlines to reply to the requests of the individuals.
4. **Number of complaints from data subjects**: 0
5. **Main issues object of complaints**: not applicable

6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: total of 303 requests (2013 - 90; 2014 - 98; 2015 - 115), among which none for rectification and 20 requests for deletion.
    a. Among those, number of requests for deletion that resulted in deletion: 6 requests; additionally, 8 requests for access that gave raise to further inquiries also resulted in deletion; therefore, there was a total of 14 alerts deleted.

7. **Number of handled cases of cooperation between DPAs:** 7 cases.
    a. Among those, number of cases which outcome was data deletion: 2.
8. **Number of inspection actions performed**: 3
9. **Raising awareness activity:** dedicated information campaign from 9 April 2013 on the second generation of the SIS: distribution of posters and leaflets and information on the DPA website. Contact with the High Commission for Migration and with some NGOs giving support to immigrants to provide them information on the rights of the individuals related to the SIS II and on the DPA's availability to welcome in our Front Office anyone who wishes to submit a request of access.
10. **Link for Schengen information in the DPA website:**
    In Portuguese: https://www.cnpd.pt/bin/direitos/schengen.htm
    In English: https://www.cnpd.pt/english/bin/schengen/schengen.htm
    In French: https://www.cnpd.pt/francais/bin/Droit/droit.htm
11. **Any relevant case-law:** none of our knowledge
12. **Any other relevant activity**: follow-up of the migration from SIS I to SIS II; development of additional cooperation mechanisms between the DPA and the SIRENE Bureau.

25. Romania

1. **Country**: ROMANIA
2. **Name of the DPA**: NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING
3. **Legal provisions implementing SIS II framework (short description):**
    In order to create the legal framework necessary for applying Council Decision 2007/533/JHA and Regulation (EC) No 1987/2006, Law no. 141/2010 on the setting up, organisation and functioning of the National Information System for Alerts (NISA) and participation of Romania to the Schengen Information System was adopted.

According to this law, the legality of the personal data processing in the N.SIS on the territory of Romania and transmitting this data abroad, as well as subsequent exchanging and processing of supplementary information are subject to monitoring and control by the National Supervisory Authority for Personal Data Processing.

According to Law no. 141/2010, the rights of the person as regards the personal data processing in the NISA or SIS II are used according to the provisions of Law no. 677/2001 on the protection of individuals with regard to the personal data processing and the free movement of such data, with the subsequent modifications and amendments, with the exceptions mentioned by this law.

4. **Number of complaints from data subjects:**
   The Romanian Data Protection Authority received 3 petitions, 1 in 2014 and 2 in 2015.
5. **Main issues object of complaints:**
   For the request submitted in 2014, the individual was asking for the deletion of an alert from the Schengen Information System concerning his vehicle. The other two requests from 2015 were referring to the exercise of the access right to the data stored in the Schengen Information System.
   In all the cases, the petitioners were recommended to address first to the national SIRENE Bureau and where the request was not handled, to address a complaint to the Romanian Data Protection Authority.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**
   Among those, number of requests for deletion that resulted in deletion
   There is a direct access.
7. **Number of handled cases of cooperation between DPAs**: no requests were received by our DPA or sent by our authority
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed:** in 2013-2015, no inspections were performed
9. **Raising awareness activity**: The website of our DPA contains a section dedicated to this subject. On this page beside the information relating to SIS II Supervision Coordination Group, the individuals have the possibility to consult/view the following: The Leaflet Schengen Information System II, the video presentation of the Schengen Information System II, as well as the Guide for exercising the right of access elaborated within the SIS II Supervision Coordination Group.
10. **Link for Schengen information in the DPA website:**
    http://www.dataprotection.ro/index.jsp?page=schengen&lang=en
11. **Any relevant case-law: -**
12. **Any other relevant activity: -**

26. Slovakia

1. **Country:** Slovak republic
2. **Name of the DPA**: Office for Personal Data Protection of the Slovak Republic
3. **Legal provisions implementing SIS II framework (short description):**
   Following legal acts govern competencies of law enforcement authorities, courts and authorities responsible for issuing visas:
   - Act No. 171/1993 Coll. on the Police Force
   - Act No 301/2005 Coll. on criminal procedure
   - Act No. 154/2010 Coll. on the European arrest warrant
   - Act No. 404/2011 Coll. on stay of the foreigners
4. **Number of complaints from data subjects:** None.
5. **Main issues object of complaints**: None.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**
   a. Among those, number of requests for deletion that resulted in deletion

   Slovak DPA does not keep a register of requests for access, correction and deletion.
7. **Number of handled cases of cooperation between DPAs:**
   a. Among those, number of cases which outcome was data deletion:

   None.
8. **Number of inspection actions performed**: 3 inspections
9. **Raising awareness activity**: Slovak DPA so far has not done any activity in this matter.
10. **Link for Schengen information in the DPA website:**
    http://dataprotection.gov.sk/uoou/en/content/schengen-area
11. **Any relevant case-law:** With regard to Slovak republic there is no relevant case-law.
12. **Any other relevant activity**: None.

27. Slovenia

1. **Country:** Slovenia
2. **Name of the DPA:** Information Commissioner
3. **Legal provisions implementing SIS II framework (short description):**
   Regulation (EC) 1987/2006 – "SIS II Regulation"
   Council Decision 2007/533/JHA - "SIS II Decision"
   The process of exercising the right to consult one's own personal data in Slovenia is regulated in accordance with the Personal Data Protection Act (Articles 30 and 31) and the Information Commissioner Act.
   In the conformity with Article 32 of the Personal Data Protection Act, the Ministry of the Interior must on the request of an individual to whom

personal data relate, supplement, correct, block or erase personal data contained in the SIS II which the individual proves as being incomplete, inaccurate or not up to date, or that they were collected or processed contrary to statute.

4. **Number of complaints from data subjects:** in period of 2013 to 2015 we didn't receive any complaint
5. **Main issues object of complaints:** /
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):** / - Police jurisdiction
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: /
    a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed**: 1
9. **Raising awareness activity:** all information about SIS II are published on website of the Information Commissioner and the Police
10. **Link for Schengen information in the DPA website:**

https://www.ip-rs.si/index.php?id=597#1203

11. **Any relevant case-law**: /
12. **Any other relevant activity:** plan the inspections on the Police and on the SIRENE Bureau

28. Sweden

1. **Country:** Sweden
2. **Name of the DPA:**
   Datainspektionen (The Swedish Data Protection Authority)
3. **Legal provisions implementing SIS II framework (short description):**
   The Schengen Information System Act (2000:344), The Schengen Information System Ordinance (2000:836) and The Personal Data Act (1998:204)
4. **Number of complaints from data subjects:** 11

5. **Main issues object of complaints:**
   Most of the complaints are request for deletion of data from SIS II.
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):**
   In Sweden the complainant should contact the Police Authority when exercising the rights mentioned above. In accordance with this, most of the complaints in question 4, has been forwarded to the police without any further action taken by the Swedish DPA. The Police Authority, as the controller, has the main responsibility to take measures against any

inaccuracies in SIS II. If the complainant is not satisfied with the result and action taken by the Police Authority, he or she may however contact the SwedishDPA. During 2013-2015 the Swedish DPA received two complaints where the complainants where unsatisfied with the reply from the Police Authority and wanted information to be deleted from SIS II. In both cases the Swedish DPA initiated inspections in writing. None of them resulted in deletion of information from SIS II.

   a. Among those, number of requests for deletion that resulted in deletion
      See above

7. **Number of handled cases of cooperation between DPAs:**
   None
   a. Among those, number of cases which outcome was data deletion:
      -
8. **Number of inspection actions performed:** 5
9. **Raising awareness activity:**
   We have updated the DPA website with relevant information about SIS II.
10. **Link for Schengen information in the DPA website:**
http://www.datainspektionen.se/om-oss/internationellt-arbete/schengen/
11. **Any relevant case-law:**
   None
12. **Any other relevant activity:**
   None

29. Switzerland

1. **Country:** Switzerland
2. **Name of the DPA:** Federal Data Protection and Information Commissioner (FDPIC)
3. **Legal provisions implementing SIS II framework (short description):**

   Federal level: The federal authorities that process personal data in the SIS must comply with the following rules:

   - The directly applicable provisions of the Schengen Convention (Title IV, particularly Chapter 3), the relevant EU legislation part of the Schengen acquis[14] of which Switzerland has been notified, the relevant acts of the Council of Europe, especially the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS

[14] According to Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (See https://www.admin.ch/opc/fr/classified-compilation/20042363/index.html).

No. 108 (28.I.1981) and its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows CETS No. 181 (8.XI.2001);

- The 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) and the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)
- Art. 13 of the Federal Constitution of the Swiss Confederation of 18 April 1999;
- The Federal Act on Data Protection of 19 June 1992 (FADP) and of the Ordinance of 14 June 1993 to the Federal Act on Data Protection OFADP);
- Art. 16 of the Federal Act on the Information Systems of the Federal Police of 13 June 2008 (FPISA) and Art. 355e of the Swiss Criminal Code of 21 December 1937 (CC);
- Federal Act of 12 June 2009 on Information Exchange between the Criminal Prosecution Authorities of the Confederation and those of Other Schengen States (Schengen Information Exchange Act, SIEA);
- The Ordinance on the National Part of the Schengen Information System and on the SIRENE Bureau of 8 March 2013 (N-SIS Ordinance).

Cantonal level: With the exception of the Federal Act on Data Protection (FADP) and the corresponding Ordinance (OFADP), the cantonal and local authorities that process personal data in the SIS must comply with the same rules as the federal authorities. Instead of the FADP and OFADP, the cantons apply their own cantonal data protection legislation.

4. **Number of complaints from data subjects**: We did not receive any complaint but we forwarded requests to the federal office of police (5 in 2013, 4 in 2014 and 6 in 2015)
5. **Main issues object of complaints:** access requests and deletion requests
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):** -
    a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs:**
   12 cases from CNIL (4 in 2013, 5 in 2014 and 3 in 2015) and 3 cases from Portugal (1 in 2014 and 2 in 2015) = 15
    a. Among those, number of cases which outcome was data deletion: 1
8. **Number of inspection actions performed:**
   On federal level, we performed five inspections:
   - Check on data security and data protection in the issuing of visas by the Swiss embassy in Dubai (United Arab Emirates);

- Information about SIS II at the federal office of police
- Elaboration of a template to analyze N-SIS log files;
- Two log files controls (Check on SIS end users)

The FDPIC also took part in the Schengen Data protection evaluations of the UK, Austria and Liechtenstein.

The cantonal data protection authorities[15] also performed 25 inspections:

- Aargau: 1 inspection
- Appenzell Inner Rhodes and Appenzell Outer Rhodes: 1 inspection each = 2 inspections
- Basel-Landschaft: 1 log files control in 2013
- Basel-Stadt: 5 inspections and some general awareness raising activities
- Bern: 1 inspection in 2015 (police)
- Geneva: one inspection in 2015 (log files) and awareness raising activity (police)
- Glarus: 3 inspections (police and migration office) including log files and access rights controls
- Neuchâtel/Jura: 3 inspections
  - SIS II and checks with national hotel registers
  - Logfiles control of some policemen
  - Check of the management of the access rights of the cantonal users
- Schaffhausen: 1 inspection (police) and several awareness raising activities
- Schwyz, Obwalden and Nidwalden: 1 control each = 3 inspections. They were focused on the access rights of the police members and internal awareness raising activities
- Thurgau: 1 inspection in 2014
- Ticino: 2 inspections

In total, **30 inspections** were performed in Switzerland.

9. **Raising awareness activity**: Keeping our website up-to-date, drafting of various documents: a factsheet on "Schengen and your personal data", model letters, a document offering an overview of the legal basis for the supervisory authorities and the remit and activities of the FDPIC in relation to the implementation of the Schengen association agreement in the field of data protection. Our annual activity report has a section dedicated to international matters. Mutual links are provided between the FPDIC and the

[15] Due to the short delay, not all cantonal data protection authorities were able to provide an answer. This information contains all the responses the FDPIC received until 2.5.2016.

federal office of police, State Secretariat for migration and federal Department of foreign affairs.

Most of the cantonal authorities now have a direct link to SIS II related information (See question 10) on their main page.

10. **Link for Schengen information in the DPA website**: http://www.edoeb.admin.ch/datenschutz/00796/00798/index.html?lang=en
11. **Any relevant case-law**: None
12. **Any other relevant activity:** None

30. United Kingdom

1. **Country:** UK
2. **Name of the DPA**: Information Commissioner's Office
3. **Legal provisions implementing SIS II framework (short description):**
   Article 4 to Protocol (No 19) to the TEU and TFEU, on the Schengen acquis integrated into the Framework of the European Union, provides that the UK may request to take part in some or all provisions of the Schengen acquis. The UK does participate in some parts of Schengen, as recorded in Council Decision 2000/365/EC (OJ L 131, 1.6.2000, p. 43–47), i.e. the police and judicial cooperation elements of Schengen and subsequently in Council Decision 2014/857/EU, which modifies Decision 2000/365/EC to include provisions concerning SIS II (OJ L 345, 1.12.2014, p. 1-5).

   The UK connected into SIS II on 13 April 2015.

   The processing of personal data under SIS II by UK authorities is governed by the Data Protection Act 1998 and Part 4 of the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014.

4. **Number of complaints from data subjects:** 0
5. **Main issues object of complaints:** n/a
6. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA)**: 0
   a. Among those, number of requests for deletion that resulted in deletion
7. **Number of handled cases of cooperation between DPAs**: 0
   a. Among those, number of cases which outcome was data deletion:
8. **Number of inspection actions performed:** 1 – post go live Audit carried out in March 2016
9. **Raising awareness activity:** Continued liaison with the National Crime Agency (competent agency for the SIRENE Bureaux)

10. **Link for Schengen information in the DPA website**: https://ico.org.uk/about-the-ico/what-we-do/international-duties/
11. **Any relevant case-law**: n/a
12. **Any other relevant activity:** n/a

Part III – The EDPS activity

This Part provides an overview of the activity of the EDPS as the supervisory authority for the central unit of SIS II.

1. **Name of the DPA:** European Data Protection Supervisor
2. **Legal provisions implementing SIS II framework (short description):**
   The SIS II Regulation and Decision describe the role of eu-LISA as management authority for the central unit of SIS II; the same texts also provide for the EDPS' role regarding the SIS II; the general tasks and powers of the EDPS are set out in Regulation (EC) 45/2001.16
3. **Number of complaints from data subjects:** 10
4. **Main issues object of complaints:**
   The EDPS has received a number of complaints concerning different kinds of alerts in the SIS. Mostly these were entry bans under Article 24 SIS Regulation which applicants found out about when visa were refused because of the alerts. As alerts are introduced by national competent authorities, complaints against specific alerts should be lodged with national DPAs. We normally referred complainants to the SIS SCG guide on access for contact details of national DPAs; where the information provided by the complainant already included information on which Member State introduced the alert, complainants were also directly referred to that Member State's DPA.
5. **Number of requests for access, correction and deletion (when these rights are exercised indirectly via DPA):** n/a
   a. Among those, number of requests for deletion that resulted in deletion: n/a
6. **Number of handled cases of cooperation between DPAs:** 1
   a. Among those, number of cases which outcome was data deletion: 0
7. **Number of inspection actions performed:**

[16] OJ L 8/1, 12/01/2001.

In spring 2015, the EDPS performed an inspection of eu-LISA as the central unit of the SIS; the inspection report was issued in autumn 2015 and follow-up with eu-LISA is ongoing.

8. **Raising awareness activity:** In October 2015, the EDPS visited eu-LISA head-quarters in Tallinn to discuss several matters related to the systems it manages.
9. **Link for Schengen information in the DPA website:** https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/IT_systems/SSIS
10. **Any relevant case-law**: n/a
11. **Any other relevant activity:**
    The EDPS and eu-LISA stay in contact regarding questions of the agency's mandate as management authority for SIS II; the SIS II SCG is kept informed via its Chair and the secretariat.

Annexes

Annex A: List of documents adopted

1. The Schengen Information System – a Guide for exercising the right of access – adopted in April 2014
2. Opinion on the Systematic checks in the SIS of hotel guests lists – adopted in May 2014
3. Report on the exercise of the rights of the data subject in the Schengen Information System (SIS) – adopted in October 2014
4. Letter to the Chair of the JSB Europol with preliminary findings about Europol's new logging system on the accesses to the SIS II: interpretation of article 45 (5)(b) of the SIS II Decision – adopted in November 2014
5. The Schengen Information System – a Guide for exercising the right of access – updated in October 2015
6. Common Audit framework: Data security model – adopted in November 2015

Annex B: List of members and observers

Members:

1. AUSTRIA:

Andrea Jelinek
Gregor König
Marcus Hild

2. BELGIUM:

Bart de Schutter
Caroline De Geest
Frédéric Claeys
Koen Gorissen

3. BULGARIA:

Desislava Toshkova-Nikolova
Mariya Mateva
Tsvetelin Sofroniev
Veselin Tselkov

4. CZECH REPUBLIC:

Frantisek Nonnemann
Klára Sommerová
Zuzana Radicova

5. DENMARK:

André Dybdal Pape
Janni Christoffersen
Morten Tønning
Sten Hansen

6. EDPS:

Achim Klabunde
Andy Goldstein
Owe Langfeld
Peter Hustinx

7. ESTONIA:

Andres Ojaver
Raavo Palu

8. FINLAND:

Heikki Huhtiniemi

9. FRANCE:

Céline Boyer
Dalila Rahmouni
Elise Latify
François Pellegrini

10. GERMANY:

Angelika Schriever-Steinberg	Hessen)
Hardy Richter	(Bonn)
Karsten Behn	(Bonn)
Nina-Verena Berg	(Hessen)
Paul Gaitzsch	(Bonn)

11. GREECE:

Elena Maragou
Ioannis Lykotrafitis

12. HUNGARY:

Dániel Eszteri
Péter Kimpián

13. ICELAND:

Thordur Sveinsson

14. ITALY:

Vanna Palumbo

15. LATVIA:

Aiga Balode
Signe Plumina (former member)

16. LIECHTNESTEIN:

Michael Valersi
Peter Bär

17. LITHUANIA:

Rita Vaitkeviciene
Neringa Kaktaviciute-Mickiene

18. LUXEMBOURG:

Thierry Lallemang

19. MALTA:

David Cauchi (Vice-Chair)

20. NETHERLANDS:

Erica Bool-Houwen

Evelien van Beek (former member)
Wilbert Tomesen

21. NORWAY:

Jörgen Skorstad
Kim Ellertsen

22. POLAND:

Anna Zawila-Niedzwiecka
Agnieszka Budzyn

23. PORTUGAL:

Clara Guerra (Chair)
Isabel Cruz

24. ROMANIA:

Alina Savoiu
Catalin Capatina
George Grigore
Georgeta Basarabescu (former member)
Oana Luisa Serghiuta

25. SLOVAKIA:

David Zubko
Ľubomír Andráš
Miroslav Rousek
Stanislav Durina

26. SLOVENIA:

Tanja Slak
Eva Kalan (former member)

27. SPAIN:

Manuel Gárcia Sanchez (former member)

28. SWEDEN:

Elisabeth Wallin

Jonas Agnvall

29. SWITZERLAND:

Caroline Gloor Scheidegger
Catherine Lennman
Veronica Blattmann
Sandra Husi (former member)

30. UK:

Alain Kapper
Hannah McCausland (former member)
Ian Williams (former member)
Jennifer Childs (former member)
Naomi Osborne-Wood

Observers:

1. CROATIA:

Marko Sijan

2. CYPRUS:

Constantinos Georgiades

3. IRELAND:

Anne Sheridan

Annex C: Members of the Secretariat

Amanda Joyce
Anne-Christine Lacoste
Evelien van Beek (former member)
Elena Jenaro Tejada (former member)
Elise Latify (former member)
Gabriela Zanfir
Gabriel Blaj (former member)
Jacob Kornbeck
Lara Smit
Lucio Scudiero (former member)
Priscilla De Locht
Raminta Sulskute (former member)