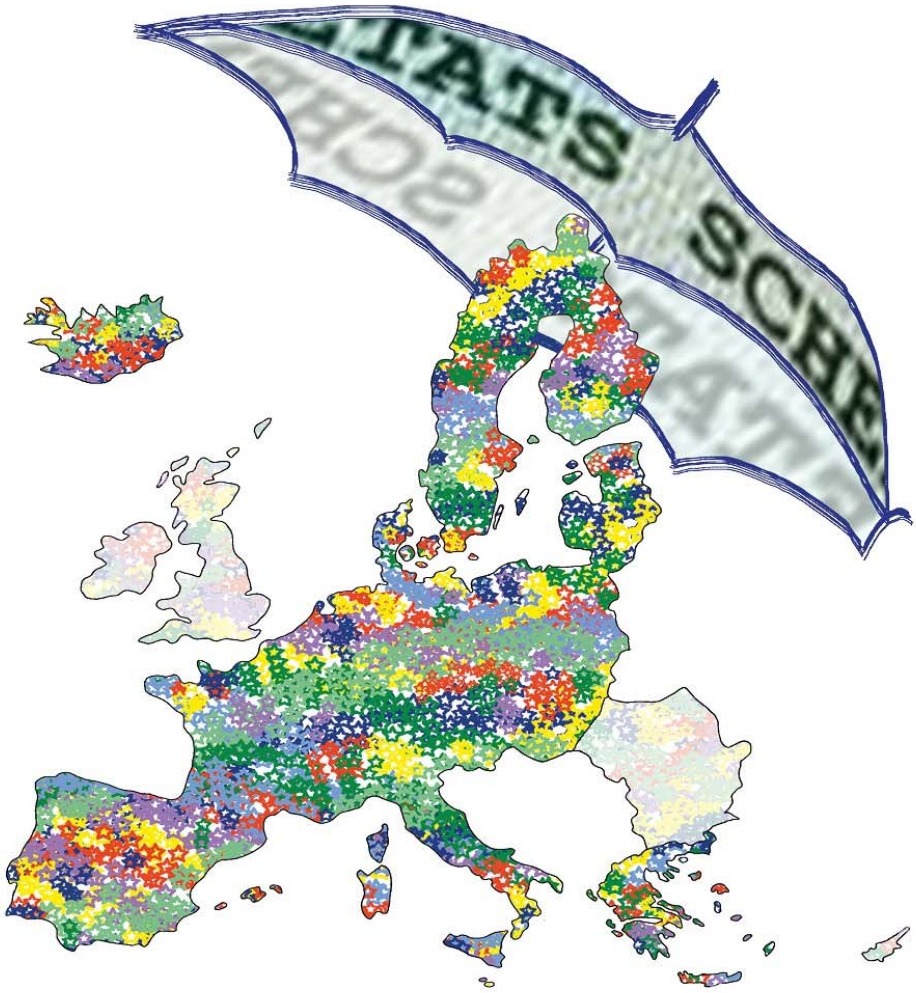
JSA ACC
SCHENGEN

SCHENGEN
JOINT SUPERVISORY AUTHORITY



NINTH ACTIVITY REPORT

JANUARY 2009 - APRIL 2013

EN

Schengen Joint Supervisory Authority

Activity Report
January 2009 - April 2013

CROSSING BORDERS

Brussels, 1 April 2013

CONTENTS

Foreword

I am pleased to present the ninth activity report of the Schengen Joint Supervisory Authority (JSA). This will be our last report. On 9 April 2013, the new Schengen Information System II (SIS II) will take over the activities of the present system. From that date, data protection supervision of SIS II will be the responsibility of the national data protection authorities and the European Data Protection Supervisor in a coordinated structure. This date also marks a period of 21 years of supervision by the Schengen Joint Supervisory Authority.

Established as a provisional joint supervisory authority in June 1992 and as the JSA on 26 March 1995 when the Schengen Convention entered into force, the JSA was the first of its kind. Creating a platform for all involved national data protection authorities to share joint responsibilities and to exchange experience, it stood as a model for the supervisory authorities of Customs Cooperation, Europol, Eurojust and Eurodac.

Now, looking back over these 21 year, one can only conclude that the JSA has proved to be an effective instrument for data protection. Effective not only in actual supervision and advising, but also in assisting citizens to use their rights.

I wish the new supervision authorities of SIS II much success and thank all who contributed to the work of the JSA.

Jean-Philippe Walter
Chair

I. About the Joint Supervisory Authority

In the village of Schengen, in 1985, the Agreement on the gradual abolition of checks at common borders was signed. In 1990, the Convention implementing that Agreement (the Schengen Convention) was signed. Today, most EU Member States, along with some non-EU countries, are part of the Schengen area[1].

Schengen provides citizens with previously-unknown freedom of movement. At the same time, Schengen States have necessarily increased controls at their shared external border to ensure the security of those living in or travelling in the Schengen Area. Success in this area requires close cooperation between Schengen States' authorities on border management. One of the key information sharing mechanisms is the Schengen Information System (SIS). The SIS allows Schengen States to exchange data on suspected criminals, on people who may not have the right to enter into or stay in the EU, on missing persons, and on stolen, misappropriated or lost property.

The SIS is the largest information system of its kind in Europe. Facilitating rapid information exchange between national border control, customs, visa, judicial and police authorities, it is one of the most important mechanisms in ensuring that the free movement of people within the EU takes place without endangering public safety.

The JSA is an independent body established[2] to ensure the protection of citizens' data protection rights in relation to the SIS.

The JSA is composed of a maximum of two members and two alternate members from each EU Member State's independent data protection authority. Each delegation has one vote. Neither the members nor the observers[3] of the JSA may sit on working groups or be members of an authority - other than the national data protection supervisory authority - instituted under the Convention. From among its members, the JSA elects a Chair and vice-Chair who serve a one-year period of office, renewable once. The JSA is supported by its own independent secretariat, based in Brussels.

The JSA holds quarterly plenary meetings in Brussels. Regrettably, several Member States were at times unable to attend JSA meetings as a direct result of financial difficulties. In 2010, the JSA found it necessary to write to the relevant government departments of one particular Member State - the Slovak Republic - to raise this issue and to highlight the fact that Member States are legally obliged to carry out their supervisory responsibilities with regard to the SIS, which includes regular attendance at JSA meetings.

---

1 Bulgaria, Cyprus, Ireland, Romania and the United Kingdom are not part of the Schengen area. Bulgaria and Romania are currently in the process of joining. Of non-EU States, Iceland, Liechtenstein, Norway and Switzerland have joined the Schengen Area.

2 Under Article 115 of the Schengen Convention.

3 The JSA may, upon unanimous decision, grant observer status without the right to vote to the representatives of the national supervisory authorities, referred to in Article 114 of the Convention, or to independent experts of the Contracting Parties who do not yet fulfill the conditions laid down in the final sentence of Article 140(2) of the Convention. A Contracting Party shall also be understood to mean a Party with which the Parties to the Schengen Agreement and the Convention have concluded a cooperation agreement on the abolition of controls at internal borders as defined in Article 1 of the Convention, provided this cooperation agreement has been ratified, accepted or approved by all Parties but has not yet entered into force.

II. Supervision

Article 115 of the Convention sets out the JSA's tasks, which are:

- to supervise the technical support function of the SIS in accordance with the provisions of the Convention, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, and in accordance with the national law of the Contracting Party responsible for the technical support function;
- to check that the provisions of the Convention are properly implemented as regards the technical support function of SIS;
- to examine any difficulties of application or interpretation that may arise during the operation of the SIS;
- to study any problems that may occur with the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of the right of access to the system; and
- to draw up harmonised proposals for joint solutions to existing problems.

Inspection
Due to the development of the Schengen II System (SIS II), the last on-site inspection was carried out in 2003. After this, the JSA shifted its supervisory focus to the content of the alerts and initiated and coordinated national inspections of the content of the SIS.

In 2005 the JSA started a project which aimed to survey the use of all categories of SIS alerts. The JSA uses a two-step approach: first, a survey based on a questionnaire in which all conditions that need to be in place to be in compliance with data protection rules when using an alert - such a survey includes a list of recommendations; and second, a check on the follow-up of the recommendations made.

Although the Schengen acquis does not aim to harmonise national practices, in the experience of the JSA, a uniform approach is required for the successful implementation of Schengen provisions concerning personal data processing. To ensure data quality and proper management and control, similar procedures and safeguards must be applied across all Schengen States.

Report of the Schengen Joint Supervisory Authority on the follow-up of the recommendations concerning the use of Article 96 alerts in the Schengen Information System, 26 November 2010
In 2005 the JSA reported on its inspection of the use of Article 96 alerts in the SIS. The report, made seven recommendations to improve the implementation of - and compliance with - Article 96 of the Schengen Convention. The report was presented to the Council of the European Union, the European Commission, the European Parliament and the national data protection supervisors.

The recommendations were:

- Policy-makers should consider harmonising the reasons for creating an alert in the different Schengen States.
- Retention periods for SIS alerts in the national sections of the SIS should be approximated in order to prevent discrepancies in the retention of alerts in the SIS.
- The appropriate national authorities responsible for Article 96 alerts should inspect these alerts on a regular basis.
- National DPAs and the JSA should further invest in developing a joint model of inspection to be used to inspect the alerts in the SIS.
- Authorities responsible for Article 96 alerts should develop formal and written procedures to ensure that Article 96 data are accurate, up to date and lawful.
- Where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organised and interlinked in such a way that data are kept accurate, up to date and lawful, and that the control of these data is guaranteed.
- Measures should be implemented or further developed to prevent Article 96 alerts on nationals from EU Member States.

The first recommendation was directed towards not only the Schengen States, but the European institutions. The other six concern the Schengen States.

As the vast majority - almost 90% - of SIS alerts are Article 96 alerts, legal compliance is critical. In 2008 the JSA Chair asked all members who took part in the 2004-2005 inspection on the use of Article 96 alerts to check the progress made at national level.

The follow-up survey identified gaps in compliance. While some Schengen states showed improved compliance, others have yet to implement the recommendations made. The JSA concluded that effective supervision and continuous attention to this issue is required from national data protection supervisors and, importantly, from the relevant national authorities.

The report on the survey was sent to the Council of the European Union, the European Commission, the European Parliament and the relevant national authorities, in order to raise awareness and highlight the areas requiring their close attention. The full report[4] can be read on the JSA website.

Inspection Report of the Schengen Joint Supervisory Authority on an inspection on the use of Article 97 alerts in the Schengen Information System, October 2009

In March 2008, the JSA decided to inspect the use of Article 97 alerts. Statistics on use indicated variations in approach by the various States. While some states barely used the article, others had entered thousands of alerts, with no apparent correlation between the size of the States concerned and the numbers of alerts entered. There also appeared to be wide differences in the numbers of alerts entered on minors.

4 http://schengen.consilium.europa.eu/reports/inspection-report.aspx?lang=en

In its inspection report[5] the JSA made seven recommendations:

- Formal written procedures should be in place for all authorities involved with entering Article 97 alerts.

- If various authorities are involved with entering Article 97 alerts, the procedures should be consistent and applied in a uniform manner.

- When the data of an alerted person are to be communicated, consent is required. The consent of an alerted person should be in writing or, at least, written proof should be available.

- In case of refusing consent this should always be in writing or recorded officially.

- Data on minors should always be controlled by automatic means and formal procedures in order to prevent that they remain alerted after the minor becomes of age.

- The M form should be used by all Schengen States.

- All Schengen States should check whether the national authorities having access to Article 97 alerts are considered authorities as referred to in Article 101(1) CISA.

Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 98 alerts in the Schengen Information System, October 2009
The competent national authorities' implementation of Article 98 was checked and, as with other inspections, the results showed differences in implementation across Schengen States. The differences concerned not only the national prerequisites for the alerts, but also the post-alert procedures.

Variations in practice were sometimes due to differences in national laws and judicial procedures. For example, the results of the survey demonstrated that the Schengen States use different retention periods for additional data exchanged via the SIRENE bureaux, even though the CISA sets out strict rules. In addition, it was clear that expired alerts were not always deleted.

The inspection also highlighted the considerable differences in the way Schengen States apply the provisions of Article 101(1) CISA concerning access to SIS data. Article 101(1) CISA states that access to data entered in the Schengen Information System and the right to search such data directly shall be reserved exclusively to the authorities responsible for:
(a) border checks; (b) other police and customs checks carried out within the country, and the coordination of such checks. The JSA questioned whether some of the authorities with SIS access actually fall within these categories.

5 http://schengen.consilium.europa.eu/reports/inspection-report.aspx?lang=en

The JSA made the following recommendations:

- In all Schengen States formal written procedures should be in place for all authorities involved with entering Article 98 alerts.
- In cases where various authorities are involved with entering Article 98 alerts, the procedures should be consistent and applied in a uniform manner.
- Improve compliance regarding data review and retention (Articles 112 and 112A CISA).
- The G form should be used by all Schengen States.
- All Schengen States should check whether the national authorities having access to Article 98 alerts are considered to be authorities as referred to in Article 101(1) CISA.

Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System, 18 December 2007

During 2006 and 2007 the JSA inspected the national competent authorities' use of Article 99 alerts. Statistics suggested the Schengen States took very varied approaches to using the system - in fact, some of them didn't seem to be using it at all - and the JSA was keen to discover why this was the case.

Though the Schengen Convention is not designed to harmonise national practices in law enforcement, the results of this inspection demonstrated a clear need for Schengen States to take a similar approach in their implementation of Article 99. A streamlined approach would provide particular benefits regarding the fulfillment of the basic principle of ensuring that data are accurate, up to date and lawful.

In its inspection report[6] the JSA made seven recommendations:

- Authorities responsible for Article 99 alerts should develop formal and written structured procedures to ensure that Article 99 data are accurate, up to date and lawful.

- There is a need for a clear definition of the types of crimes that can lead to an Article 99 alert. Although the new legal basis for SIS II contains the general term "serious criminal offences," it is suggested to agree on a European level to a uniform interpretation of the term "serious crime." The list of serious crimes for which Europol is competent or the Council Framework Decision on the European Arrest Warrant can be used for this purpose.

- The appropriate national authorities responsible for Article 99 alerts should better control and inspect these alerts every six months. Additional guidelines should be set out.

- The list of authorities (including also the national security services) that have access to Article 99 alerts should be harmonised in all EU Member States.

- Where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organised and interlinked in such a way that data are kept accurate, up to date and lawful, and that the control of these data is guaranteed.

- An alert concerning contact persons is not permissible in view of the wording of Article 99(2).

- National data protection authorities should inspect Article 99 alerts periodically.

6 http://schengen.consilium.europa.eu/reports/inspection-report.aspx?lang=en

The follow-up survey identified that most participating Schengen States must still invest in cooperation procedures in the area of law enforcement at national level to ensure that all conditions are in place allowing an Art. 99 alert to be made. While the procedures when reviewing these alerts – either after six months or close to the retention period – may be sufficient, this is not the situation preceding the alert.

Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 95 alerts in the Schengen Information System, 19 March 2013

The objective of the inspection was to ensure that Article 95 data are processed in accordance with Article 95 and the data protection principles in the Schengen Convention, the SIRENE Manual and the applicable national legislation. The inspection was also designed to enable the JSA to assess whether there are any interpretation problems with the use of Article 95.

This report was finalised just before the new legal basis for SIS II becomes applicable. As Article 26 of Council Decision 2007/533/JHA covers the same type of alerts, the report, its conclusions and recommendations will be valuable for these alerts in SIS II.

The results of this inspection demonstrate that while, in general, the implementation of Article 95 alerts and EAWs may be in compliance with the legal basis, there are too many examples where the process of alerting, maintaining the alert, having data up to date and correct, and the communication of information, are not in line with the legal basis and must be improved.

The results show that not all Schengen States act in compliance with Article 95(2). As the obligation of that paragraph does not appear in the new legal basis for SIS II, the JSA did not formulate a recommendation in this respect. An important conclusion was that all authorities involved with issuing and distributing an EAW should act in compliance with their responsibilities. The inspection demonstrated that not all parties in the chain of responsibilities for using an Article 95 alert always act as they should.

Recommendations made:

- Harmonise the data to be transferred when an arrest cannot be made and the person is found.
- Centralise the responsibility for changing inaccurate data, for example with the SIRENE bureaux to prevent lengthy procedures for changing the data.
- Better implement the obligation for having the documentation available in accordance with the SIRENE Manual before issuing the alert.
- Better implement the obligation to delete the alert directly after arrest and surrender.
- Develop harmonised guidelines for the deletion of an alert after a certain period of inactivity. These guidelines should differentiate between the reasons for inactivity.
- A definite decision to maintain or delete an alert must be made during the three-year review.

Opinions issued during the period covered by this report

Opinion on the systematic verification in the National Schengen Information Systems (NSIS) of guests staying in Schengen State hotels: compliance with the Schengen Convention, March 2011

The JSA's opinion on the use of the Schengen Information System for cross-checks with national hotel registers noted that the Schengen Convention does not explicitly forbid the use of automated verification techniques when checking whether persons are alerted in the Schengen Information System using the content of another file. But this kind of verification is only possible within the limits of Article 102 of the Convention, which deals with the purposes for which the alert data may be used.

A Schengen State may use verification techniques to verify whether a person subject to a check or control is alerted in the SIS; however, verification and use is limited to the purpose of the alert and the check or control activity should obey national law. Verification techniques should also comply with the principle of proportionality.

In Schengen States, information collected for hotel registers will be used for verification. This information includes data about guests - with the exception of accompanying spouses and minors - and may be used when necessary for the prevention of threats, for criminal investigations or for clarifying the circumstances of missing persons or accident victims. Limits are placed on the categories of data processed in these registers and the purpose of the use of these registers by authorities.
The JSA formed the opinion that in view of the content of the SIS, the limitations on the legal purposes of using SIS alerts, and the grounds for using hotel registers, automatic verification against all SIS alerts using hotel registers is not in compliance with the Convention.

Article 45(1)(b) of the Convention does, however, provide the possibility for national law to allow deviation from the conditions for using the hotel registers (providing these deviations do not contradict the conditions for the use of SIS data). Even if such deviations allow the possibility to verify these hotel registers with the content of the SIS, this would only be legitimate if use is: in compliance with the purposes of the alerts; necessary; and proportionate. This means that continuous, full, systematic verification of hotel registration forms with the SIS is not possible.

Opinions on the implementation of Article 102A of the Schengen Convention

Under Article 102A(4) of the Convention, the Council must submit to the European Parliament a report on the implementation of Article 102A of the Convention, and specifically on the implementation of the applicable data protection rules, after seeking the opinion of the JSA.

The JSA's October 2009, March 2011 and October 2012 opinions are similar in nature, highlighting the fact that the Council's reports, to date, do not contain the necessary information to allow a meaningful assessment of compliance with the data protection rules. The JSA found that the information contained in the Council's reports was not sufficient to enable a proper assessment of the implementation of Article 102(A). Other important issues highlighted included the lack of harmonisation across Member States in terms of how they have implemented Article 102(A); and apparent problems in various Member States with logging use of the system, and with collecting relevant statistics.

Other activities

Schengen catalogue: data protection recommendations and best practices, 2009
This catalogue was developed to help the data controllers of the N-SIS in each Member State to uniformly implement standard requirements on personal data protection in practice. It also provides the national supervisory authorities with defined criteria for the use in their inspections at national level.

Data protection practice issues in external representations and their service providers, December 2012
Following an exchange of views within the JSA on the outcomes of inspections of external representations (embassies, consulates) and their service providers, the JSA contacted the Council, Commission, European Parliament and the national data protection authorities to draw their attention to the problems identified.

Problems included data security, staff awareness, the use of blacklists, and the need for sufficient clauses in contracts between external representations and their service providers to ensure data protection.

Resolving citizens' problems
Citizens have a number of rights under the Schengen Convention.

- To access information concerning them which is contained in the SIS
- To correct or delete their personal information if there is a factual mistake or if certain legal requirements have not been met
- To apply to the courts or the competent authorities to demand that their personal information be corrected or deleted, or that damages be awarded
- To ask for their personal information to be checked and question the use of the information

To exercise these rights, citizens must apply to a national supervisory authority that is competent for supervision of the national part of the SIS (the N.SIS) or directly to the authority handling the data (police, customs authorities, etc.).

In addition to these rights, citizens can ask the national authorities to ensure that the manner in which their personal information was collected, stored, processed and used by in the SIS is lawful and accurate.

To help citizens to exercise their rights, the JSA website contains guidance and model letters. The JSA started a survey on the practice at national level of the right of access; the results are expected mid 2013.

Transparency
The JSA is obliged to submit regular activity reports to the authorities to which the national data protection supervisory authorities submit their reports. Transparency is fundamental to our work so, in addition to presenting our activity reports, we publish, where possible, our documents on our website[7] in order to inform the public and other practitioners about our work. Our Rules of Procedure[8] regulate public access to our documents.

---

7 http://schengen.consilium.europa.eu

8 approved by the JSA on 2 February 1996, Article 2 of which was amended by the JSA's decision at its meeting of 4 July 1997 and amended on 27 April 1998 by the addition of a new Article 11

JSA impact on supervision at national level
The work of the JSA, as with the other data protection joint supervisory authorities, has a positive impact on data protection at national level. Being composed of data protection experts from each EU Member State's data protection authority provides a two-way benefit: the JSA creates, through the collective knowledge and experience of all Member States' data protection supervisors, harmonised approaches to law enforcement issues. In particular, experience gained during on-site inspections leads to further harmonisation of national practices in assessing data before they are inputted into SIS. Joint decisions of the JSA are applied at national level. This is a key advantage of joint supervision.

Other activities
The JSA participated in the Working Party on Police and Justice (WPPJ), an advisory group of European data protection authorities, until the European Privacy and Data Protection Commissioners' Conference (known informally as the Spring Conference) ended its mandate in 2012.

III. Looking towards the future

Developing the second generation SIS - SIS II
Work on SIS II is ongoing. This new system will have enhanced capabilities, involving biometrics, new types of alerts, the ability to link various alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. It is hoped that it will also ensure stronger data protection. The new system will be implemented in April 2013.

SIS II will comprise a central system, EU States' national systems and a communication network between the central and the national systems. The European Commission is responsible for the development of the SIS II central system, while SIS II national systems are being developed by the Schengen States. Once operational, SIS II will be managed by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. The Agency will take the form of an independent European body - a regulator. In addition to SIS II, the Agency is tasked with managing EURODAC and the Visa Information System.

The future of supervision
In the wider scheme of things, the Lisbon Treaty abolishes the former three-pillar EU structure and brings justice and home affairs under the umbrella of 'freedom, security and justice'. Its entry into force will lead to the development of one data protection framework across all areas of EU activity, including the former 'third pillar' - the police and judicial cooperation area. The specific data protection rules which exist in the area of police and judicial cooperation are set out in the relevant legal frameworks: for example, the Europol Council Decision, the Eurojust Decision, the Customs Decision, and the Schengen Convention. The rules are designed to take into account the particular, and often very sensitive, nature of the data processed, and the possible high risks posed to citizens; they also ensure close supervision of the concerned systems and organisations.

The European Commission presented on 25 January 2012 its proposal for the future EU data protection legislative framework, consisting of a general data protection regulation and a directive for data processing in the area of law enforcement. The proposals are in line with the Commission's communication 'A comprehensive approach on personal data protection in the European Union' of 4 November 2010, which states, 'The Commission stresses that the notion of a comprehensive data protection scheme does not exclude specific rules for data protection for the police and the judicial sector within the general framework, taking due account of the specific nature of these fields'. The Council of the European Union's conclusions on the Commission's communication emphasise 'the need to establish specific data protection rules for the sector of police cooperation and judicial cooperation in criminal matters in conformity with the Charter of Fundamental rights.'

The proposals for the future legal framework will not apply to SIS II and other forms of law enforcement cooperation such as within Europol and Eurojust.

The JSA has participated in the discussion on the future of supervision in the police and judicial cooperation area. Over the past years, we jointly organised and participated in several plenary meetings with the joint supervisory bodies of Europol, Eurojust and the Customs Information System to specifically discuss this issue.

Chair and members of the JSA are also part of an expert working group set up during the 2011 European Privacy and Data Protection Commissioners' Conference to focus on the future of supervision in the freedom, security and justice area, particularly with regard to what makes supervision effective. The group held its first meeting in June 2011 and continued to meet quarterly. In early 2013, the group finalised a report on the future of data protection supervision in the area of law enforcement, which explains its vision for the future. In May 2013 this report will be discussed in a conference of all European data protection authorities.

IV. Budget

The JSA is granted a budget, shown as a separate budget heading in the general Schengen budget, which enables the authority to implement its annual work programme in accordance with the tasks conferred upon it by the Convention. The JSA decides on the disbursement of its budget, which is administered by the secretariat.

V. Members, alternates and observers

Austria
Mr Gregor KÖNIG
Mrs Eva SOUHRADA-KIRCHMAYER
Mr Marcus HILD

Belgium
Mr Frederic CLAEYS
Mr Koen GORISSEN
Mr Bart de SCHUTTER

Czech Republic
Mr František NONNEMANN
Mrs Zuzana RADICOVA

Denmark
Mr Janni CHRISTOFFERSEN
Mr André DYBDAL PAPE

Estonia
Mr Andres OJAVER

Finland
Mr Reijo AARNIO
Mrs Elisa KUMPULA
Mr Heikki HUHTINIEMI

France
Mrs Dominique CASTERA
Mrs Dalila RAHMOUNI
Mr Emile GABRIE

Germany
Mr Michael RONELLENFITSCH
Mrs Angelika SCHRIEVER-STEINBERG
(Chair, 2010-2012)
Mrs Gabriele LÖWNAU
Mr Karsten BEHN

Greece
Mrs Eleni MARAGOU
Mr Ioannis LYKOTRAFITIS
Ms Efrosini SIOUGLE

Hungary
Mr Peter KIMPIAN
Mrs Julia SZIKLAY

Italy
Mrs Vanna PALUMBO

Iceland
Mr Bjorn GEIRSSON
Mrs Sigrun JOHANNESDOTTIR
Mr Thórdur SVEINSSON

Latvia
Mrs Signe PLUMINA
Mrs Aiga BALODE

Liechtenstein
Mr Philipp MITTELBERGER
Mr Peter BAER

Lithuania
Mrs Rita VAITKEVIČIENĖ
Mrs Barbara JURGELEVIČIENĖ

Luxembourg
Mr Pierre WEIMERSKIRCH
Mr Thierry LALLEMANG
Mr Georges WIVENES

Malta
Mr Joseph EBEJER
Mr David CAUCHI

Netherlands
Mr Mr Jacob KOHNSTAMM
Mr Wilbert TOMESEN
Mr Paul BREITBARTH
Mrs Evelien VAN BEEK

Norway
Mr Kim ELLERTSEN
Mrs Cecilie RØNNEVIK

Poland
Mr Wojciech WIEWIÓROWSKI
Mr Piotr DROBEK

Portugal
Mrs Isabel CRUZ
Mrs Clara GUERRA
Mr Luis BARROSO

Slovakia
Mr Stanislav ĎURINA
Mrs Zuzana VALKOVÁ

Slovenia
Mrs Natasa PIRC MUSAR
Mrs Eva KALAN

Spain
Mr Rafael GARCÍA GOZALO
Mr Manuel GARCÍA SÁNCHEZ

Sweden
Mr Nicklas HJERTONSSON
Mrs Cecilia BERGMAN
Mrs Elizabeth WALLIN
Mr Jonas AGNVALL

Switzerland
Mr Jean-Philippe WALTER (Chair, 2012-present)
Ms Sandra HUSI
Ms Catherine LENNMAN
Ms Veronika BLATTMANN
Mr Michele ALBERTINI

Observers

Bulgaria
Mrs Mariya MATEVA
Mr Veselin TSELKOV
Mr Valentin ENEV

Ireland
Mr Gary DAVIS
Mrs Eunice DELANEY
Mrs Anne SHERIDAN

United Kingdom
Mr Ian WILLIAMS
Mrs Hannah McCAUSLAND

Cyprus
Mr Yiannos DANIELIDES
Mr Ioanna ANASTASIADOU
Mr Constantinos GEORGIADES

ROMANIA
Mrs Georgeta BASARABESCU
Mr George GRIGORE

VI. Key legal texts

- 09/05/2008 - Protocol integrating the Schengen acquis into the framework of the European Union

- 22/09/2000 - The Schengen acquis, as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999, including the Schengen Agreement and the Schengen Convention

- 19/06/1990 - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders

SIRENE Manual

- 01/07/2011 - Commission Implementing Decision 2011/406/EU of 1 July 2011 amending the SIRENE Manual

- 04/03/2008 - Commission Decision 2008/334/JHA of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II)

- 04/03/2008 - Commission Decision 2008/333/EC of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II)

Second generation Schengen Information System

- 05/11/2010 - Report from the Commission to the European Parliament and the Council - Progress Report on the development of the second generation Schengen Information System (SIS II) - January 2010 - June 2010 (COM(2010) 633 final)

- 06/05/2010 - Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report July 2009 - December 2009 (COM(2010) 221 final)

- 22/10/2009 - Report from the Commission to the Council and the European Parliament on the development of the second generation Schengen information system (SIS II) - Progress Report January 2009 - June 2009 (COM(2009) 555 final)

- 24/03/2009 - Report from the Commission to the Council and the European Parliament on the Development of the Second Generation Schengen Information System (SIS II) - Progress Report July 2008 – December 2008 (COM(2009) 133 final)

- 12/06/2007 - Council Decision No 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

- 20/12/2006 - 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)

Migration from SIS 1+ to SIS II

- 17/09/2009 - Commission Decision 2009/724/JHA of 17 September 2009 laying down the date for the completion of migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)

- 17/09/2009 - Commission Decision 2009/720/EC of 17 September 2009 laying down the date for the completion of migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)

- 24/10/2008 - Council Regulation (EC) No 1104/2008 of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (consolidated version of June 2010)

- 24/10/2008 - Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (consolidated version of June 2010)

Information management in the Freedom, Security and Justice area

- 20/07/2010 - Communication from the Commission to the European Parliament and the Council - Overview of information management in the area of freedom, security and justice (COM(2010) 385 final)

European Agency for large-scale IT systems

- 25/10/2011 - Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

- 14/12/2010 - Council Decision 2010/779/EU of 14 December 2010 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice