REPORT

Schengen Joint Supervisory Authority
Activity Report – December 2005 – December 2008

Table of Contents

Foreword 3
1. Introduction 4
2. New developments: SIS II 5
2.1 The migration from SIS I+ to SIS II 7
2.2 Enlargement of the Schengen Area 9
3. Supervisory work 11
3.1 Article 99 inspection 11
3.2 Article 111 survey 14
3.3 Follow-up of Article 96 inspection 18
4. Opinions of the Joint Supervisory Authority 21
4.1 Interpretation of Article 111 of the Schengen Convention 21
4.2 Opinions on the implementation of Article 102A (SCHAC 2501/07)/ SCHAC 2504/08 25
4.3 Opinion on the implementation of a mail server relaying SIRENE messages in a central point in C.SIS premises (SCHAC 2502/07) 27
4.4 Opinion on the draft implementing measures including the SIRENE Manual for the second generation Schengen Information System (SCHAC 2503/07) 28
4.5 Opinion on the principles governing cooperation between national supervisory authorities based on the Schengen Convention 31
4.6 Opinion on the Schengen Information System and violent troublemakers 08/10 32
5. Data subjects' rights 35
6. Future of joint supervision 37
7. Members of the Schengen Joint Supervisory Authority 39
8. Observers of the Schengen Joint Supervisory Authority 41

Foreword

The Schengen area can be regarded as a major achievement in creating an open-border space in Europe. All persons in that area are directly concerned with the issues of their security and of respect for their private life and their rights, including the right to protection of their personal data.

All the national data protection authorities working together in the Schengen Joint Supervisory Authority have shown their determination to protect the privacy of the individual in respect of the enormous amount of personal data processed in the Schengen Information System.

During this three-year period (December 2005 - December 2008), we have focused on the correct interpretation of the Schengen Convention and assessed whether the Schengen States have implemented this legal framework in a harmonised and appropriate manner.

Sharing the common aim of providing persons with a high level of security through specific border and other controls in the Schengen area, the Schengen States have also developed various new policies in the area of immigration control and the fight against serious crime. These new developments have led national data protection authorities to improve their cooperation and to introduce benchmarking of best practices. The JSA has expressed its concern about some of these new developments.

Two major challenges now face us: the enlargement of the Schengen area, accentuating the need for better harmonisation between all the Schengen States, and the development of the second generation of the Schengen Information System (SIS II) including the complex migration from the present system to the new one.

This report also shows the work done by all the national data protection authorities, and the secretariat's first-rate contribution to promoting better harmonisation and better understanding between us.

Our biggest challenge remains responding to all the developments in the fight against crime and illegal immigration, in promoting a European space of justice, in improving the level of security for all the persons by detecting risks of terrorism and serious crime and to striking a good balance between security and privacy.

Georges de LA LOYERE
Chairman of the Schengen Joint Supervisory Authority

1. INTRODUCTION

Citizens of the European Union enjoy the right to travel freely from one country to another. Although this right dates from the start of the EU, the abolition of internal borders in the EU by the Schengen Agreement has turned this right into a reality and offered greater freedom of movement, a privilege for EU citizens. The need to find an adequate substitute for those borders to ensure that the EU remained an area of freedom, security and justice was evident. The abolition of one safeguard resulted in the creation of another – the Schengen Information System – to process the personal data of individuals in order to maintain public order and security, including national security, in the territories of the Schengen States, and to apply the provisions of the Convention relating to the movement of persons in those territories, using information communicated via that system. It is probably fair to say that the Schengen Information System was the predecessor of all present and future large-scale EU information systems creating a data surveillance network in the EU. The most recent example, namely the systems introduced by the Treaty of Prum, to a great extent mirror the design and functions of the Schengen Information System, although in principle they focus on EU citizens. Recently, many measures to facilitate the exchange of information have been adopted without the necessary assessment of the existing systems and of the possible impact on the protection of the rights of individuals - not only the right to privacy and the right to data protection, but also the freedom of movement of persons and the principle of non-discrimination.

The Schengen Convention established the Joint Supervisory Authority, an independent body charged with inspecting the central section of the Schengen Information System, examining any difficulties of application or interpretation in the operation of the system, and ensuring that the system complied with the relevant provisions on data protection.

This activity report, the eighth by the Joint Supervisory Authority, provides an overview of its commitment and involvement in the development of the second-generation Schengen Information System (SIS II), the Joint Supervisory Authority’s role during the enlargement process, and its initiatives for joint activities together with national data protection authorities concerning the compliance of personal data entered in the SIS for alerts under Article 99 of the Schengen Convention, including the report on the survey of the implementation of Article 111 of the Schengen Convention. The report also reflects on the activities of the Joint Supervisory Authority in dealing with complaints by individuals, the Authority's opinions on various data protection questions and the future prospects for joint supervision of the SIS.

2. NEW DEVELOPMENTS: SIS II

The Joint Supervisory Authority, which has been closely involved in monitoring the development of the second generation of the Schengen Information System (SIS II), provided guidance and assistance to the EU institutions, aiming to assure that the SIS II would comply with the necessary data protection standards. In September 2006 the Joint Supervisory Authority issued its opinion on the proposed legal basis for SIS II.

The Joint Supervisory Authority's contributions to the development of SIS II date from 2004. In its opinion of 19 May 2004 on the future development of SIS II the Joint Supervisory Authority outlined some principal concerns, and actions that should be taken. In October 2005, the Joint Supervisory Authority delivered an opinion on the proposed legal basis for SIS II, based on a draft Regulation[1] and a draft Decision[2], in which it systematically evaluated the new architecture of the system in relation to the existing and proposed new data protection framework. The Joint Supervisory Authority made many detailed remarks and suggestions to improve the draft legal texts. Since then, the new proposals for the legal basis for SIS II have been continuously under discussion at the Council and the European Parliament, leading to many amendments to the original proposals. The Joint Supervisory Authority addressed some important issues in relation to the revised proposals from the Finnish Presidency[3] of 27 July 2006 on the establishment, operation and use of SIS II. By doing this, it contributed to the improvement of the legal basis from a data protection point of view. In its opinion the Joint Supervisory Authority welcomed limiting the role of SIS II to its compensatory role, as this seemed to be an important step towards the limitation of the purpose of SIS II as advocated by the Joint Supervisory Authority. It underlined that the intended technical requirements to be developed for SIS II, in view of their impact on individuals, must never reduce the level of data protection. The Authority underlined its strong wish to be involved during the transitional period, in particular in the light of the establishment of the Management Authority. The Joint Supervisory Authority raised some concerns on the use of biometric data in SIS II and welcomed certain limitations on the use of such data, pointing out that biometric data could be regarded only as an additional tool to verify the identity of the person concerned, if the technical quality requirements to be developed were adequate and contained the necessary safeguards. Unconditional use of biometrics for identification purposes would no doubt lead to the use of this functionality by an increasing number of authorities for various purposes. Such "function creep", also taking into account the desire for interoperability between SIS II, VIS and Eurodac, should be

[1] COM (2005) 236, 2005/0106 (COD).
[2] COM (2005) 230, 2005/0103 (CNS).
[3] 5709/9/06 and 5710/5/06.

prevented. In its opinion, the Joint Supervisory Authority suggested adding a provision in the proposals stating that the use of biometrics to identify a person was to be strictly limited to the purposes of the alerts. The Joint Supervisory Authority concluded that biometric data (fingerprints) processed in the SIS II should only be used to verify the identity of the person concerned: limited to the purpose of the alerts, and not extended to other identification searches. Technical developments to be used for one-to-many comparison should, due to the intrinsic nature of fingerprints, not only be of the highest standard but should also include a remedy for the individual. The use of such comparison should furthermore not be an option chosen solely on technical grounds, but should also require an assessment of necessity and proportionality, given the impact it would have on individuals' rights. The Joint Supervisory Authority insisted that the mechanisms must ensure that the data were accurate and lawfully processed, in order to safeguard citizens' rights. The Joint Supervisory Authority also proposed that the texts of the proposals should be amended in such a way that cases of dispute between the Member States were submitted to the appropriate coordinated supervision of SIS II.

Already before the start of the discussions on SIS II it appeared that there was a strong wish to grant Europol and Eurojust access to some specific alerts that could be useful for the fulfilment of their tasks. In all its opinions, the Joint Supervisory Authority warned that such access should not lead to routine access by these organisations. The alerts which they are entitled to access did not necessarily contain information which fell within the objectives of Europol and Eurojust. Regulation (EC) No 1987/2006, Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Regulation (EC) No 1986/2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates were adopted, and formed the legal basis for the activities of the SIS II as well as laying down the rules on the data protection and data protection supervision regime.

2.1 The migration from SIS I+ to SIS II

With the increased number of Member States of the European Union after the Union's enlargement, it became clear that the SIS must be designed to handle more than double the number of Member States dealt with by the current SIS. At the same time, the question of the migration of data from SIS I+ to SIS II and preparatory works drew the attention of the Joint Supervisory Authority. At this stage it was important to ensure that during the migration of data from one system to another, important data protection principles (the integrity of the data, the confidentiality of the data, the purpose) should be respected.

On 19 April 2006 the Joint Supervisory Authority received a request from the Chairman of the Article 36 Committee to review the proposed rules for the production of a SIS I+ test database in order to prepare for the migration from SIS I + to SIS II.

Although fully supporting the creation of the test database for SIS II, the Joint Supervisory Authority noted in its Opinion 06–05 that the data fields in the proposal could by accident produce the data of real persons, and that therefore some additional security measures should be applied. In its opinion, the Joint Supervisory Authority also highlighted that the use of personal data as test data during the development of information systems posed a number of risks. When creating test data for an information system like SIS II, it was generally accepted that the creation of such test data should follow the concept of privacy-preserving data migration: developing accurate models without access to precise information in individual data records, thus resolving the conflict between privacy and data migration. Anonymisation techniques should allow the use of data sets without disclosing identity. The Authority noted that privacy-preserving data migration should rely on the notion that one's personal data could be protected by being scrambled or randomised prior to being communicated. By applying a specific technique, highly accurate data models could be generated without disclosing personal information. The Joint Supervisory Authority noted that in the presentation of the proposal, it was admitted that in the test data that would be produced, there was the possibility that real data would be revealed. Since the proposal left the name (first name and surname) fields unchanged and only made inter-exchanges between similar records, there was a great risk that individuals could be identified. It was admitted that recognising this risk, the proposal introduced some extra procedural measures to restrict the use of the test database. However, these measures would never prevent disclosure to third parties. The Joint Supervisory Authority supported the extra measures as a general

extra safeguard, but pointed out that they could not replace the need for test data to be rendered completely anonymous. It also provided a number of recommendations concerning the development of special security policies, the avoidance of the use of sensitive data in test environments, the methodology for anonymisation, the logging of access to test data, the provision of audit trails even for the Joint Supervisory Authority, and time-limits for the use of this test database.

In April 2008 the Commission submitted two proposals on a Council Regulation and a Council Decision on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) in order to establish the legal framework governing the migration from SIS 1+ to SIS II. On 30 June 2008 the European Parliament Committee on Civil Liberties, Justice and Home Affairs organised a Round Table on Freedom and Security in the Integrated Management of the EU's Borders, including the session "*SIS II: When; Why; How?*". The Chairman of the Schengen Joint Supervisory Authority attended the event and contributed to discussions on the data protection implications of the migration from SIS I to SIS II. In October 2008 the Council adopted the Council Decision and Council Regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II).

2.2 Enlargement of the Schengen Area

One of the important events during the period 2005–2008 which deserves to be mentioned was the enlargement of the Schengen Area, allowing nine new Member States to join the Schengen Area and their citizens to fully enjoy the freedom to cross internal borders without having to show passports or identity cards, except for travel to the UK, Ireland and Cyprus, plus Bulgaria and Romania, which only joined in 2007. The long process of Schengen evaluation visits and re-visits lasted for 2 years. The evaluation consisted in particular of verifying that the accompanying measures allowing for the lifting of internal border control were being correctly and efficiently applied by the new Member States. Evaluation visits were carried out in the field of external border control, visas, data protection, police cooperation and the Schengen Information System.

The development of SIS II was related to the creation and implementation of the new functionalities within the System (reinforcing security and making more efficient use of data), also making the system technically able to serve more than 18 countries. The delays in launching the new system and the need for the new Member States to join the system as soon as possible forced Member States to find a quick alternative solution. In December 2006 the Council decided to implement Portugal's SISone4ALL proposal to integrate nine of the Member States which joined the European Union in May 2004 into SIS 1+ temporarily. The aim of the SISone4ALL project was to facilitate the process leading to the lifting of internal border controls with the Member States concerned between December 2007 and March 2008. In accordance with Council Decision 2007/471/EC of 12 June 2007, the Member States were able to enter data into the SIS and use SIS data from 1 September 2007.

On 21 December 2007, Estonia, the Czech Republic, Lithuania, Hungary, Latvia, Malta, Poland, Slovakia and Slovenia became part of the Schengen area. On 30 March 2008 the enlargement process was completed by lifting air border controls between these countries and with the 15 states that were already part of the Schengen system.

Even before enlargement, the SIS was one of the most important and biggest databases used for immigration and border controls in the EU. On 1 January 2007 the total number of valid records in the SIS was 17 615 945. After the nine new States joined the Schengen area and began operation of the SIS on 1 January 2008 this number increased to 22 933 370 valid records. In total the number of valid records in the database increased by 23 % during this period. Comparing the statistics on 1 January 2008 with 2007[1], the biggest increase in records containing personal data was for ID (issued documents), where numbers increased from 13 752 947 to 17 876 227 (23%). The statistics

[1] 5441/08, 30 January 2008; 6178/07, 13 February 2007.

are as follows (by Article of the Schengen Convention):

Art. 95 (wanted for arrest/extradition)	+ 16%
Art. 96 (unwanted alien)	- 7,4%
Art. 97 (adult missing person)	+ 14%
Art. 97 (minor missing person)	+ 6,8%
Art. 98 (localisation)	+ 22%
Art. 99.2 (check/observation)	- 5%
Art. 99.3 (check/observation)	- 22%

The reduced number of alerts on unwanted aliens could be explained by the simple fact that due to the accession of the new Member States to the EU, the citizens of those states became EU citizens, and therefore the records on those persons should have been deleted from the system. In view of this, the initiative of the Joint Supervisory Authority to follow-up the inspection of Article 96 was timely and the results were satisfactory. From the answers received, no cases of the processing of data of EU citizens under Article 96 were reported. However, due to the low number of answers received, it is evident that this work needs to be done in all the Schengen States.

The enlargement also meant an increase in the number of members of the Joint Supervisory Authority. These new members were already participating as observers in the work of the Joint Supervisory Authority, thus gaining a great deal of knowledge in preparation for their new tasks and duties. By granting this observer status, the Joint Supervisory Authority played an important role in raising the awareness and knowledge of the future members, giving opinions and advising on questions received from the observers concerning various interpretations of the provisions of the Schengen Convention. At the same time, the experience of the new members which they gained through the long preparation and evaluation process (participation in the preparatory work for the SIS national legislation, *a priori* audits of the IT systems, consultative work with the competent institutions, awareness-raising campaigns on the rights of the individuals in the SIS, supervisory work in consulates, police authorities, etc.) was of great importance to the so called "old members" of the Joint Supervisory Authority.

All this is of great value for the joint coordinated work supporting the effective protection of the rights and freedoms of individuals and the future supervision of SIS II.

3. SUPERVISORY WORK

Article 115(3) of the Schengen Convention stipulates that the Joint Supervisory Authority shall also be responsible for examining any difficulties of application or interpretation that may arise during the operation of the Schengen Information System, for studying 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 for drawing up harmonised proposals for joint solutions to existing problems. To implement this provision of the Convention in practice, the Joint Supervisory Authority chose to conduct inspections at national level. The obvious practical benefit of such activities was insight and knowledge of how the Schengen States were implementing and using the Articles of the Schengen Convention, and an overview of practical problems that may occur with implementation.

3.1 Article 99 inspection

One of the main characteristics of the Schengen Information System is the shared responsibility for the use of the system, in accordance with the provisions set out in the Schengen Convention and in national laws. It is fair to say that the Schengen Joint Supervisory Authority was the first supervisory authority which promoted joint coordinated supervisory activities in the law enforcement area as regards the inspection of large-scale databases. This new approach to the supervisory role was indeed successful, inspiring future coordinated supervision. This system of surveys provided significant help with the harmonisation of the implementation of the Schengen Convention and the use of the SIS.

In June 2006, the Schengen Joint Supervisory Authority asked national data protection authorities to inspect Article 99 alerts entered in the Schengen Information System (SIS) by their competent authorities.

This was the second survey initiated by the Joint Supervisory Authority on the use of a specific Article of the Schengen Convention (*e.g. concerning Article 96 in the year 2005*). Often the results indicated various differences between the Schengen States enabling the Joint Supervisory Authority to draw conclusions and to recommend the necessary measures.

The objective of the inspection was to ensure that Article 99 data were processed in accordance with Article 99 and with the data protection principles in the Schengen Convention, the SIRENE Manual and the applicable national legislation. The method of the inspection made it possible for the Joint Supervisory Authority to assess whether interpretation problems existed in the use of Article 99.

For that purpose, the Joint Supervisory Authority developed a simple method of inspection to be used equally by all national data protection authorities. A comprehensive questionnaire was developed. This questionnaire aimed to get an overview of the relevant national law in the Schengen States and to check that all the necessary procedures were in place for the authorities responsible for the alerts to fulfil the data protection requirements. It also contained specific questions to check whether the alerts were in accordance with the provisions of Article 99 and whether they were maintained in the SIS in accordance with the provisions laid down in the Schengen Convention.

The joint effort of the national data protection authorities, to check the national Article 99 contributions to the SIS in a certain period and using the same model for inspection, once more emphasised a joint concern for the proper use of the SIS. This second joint action was again a milestone in cooperation between national data protection authorities in the European Union and underlined the need to invest in establishing a framework for data protection inspections in those areas where cooperation between Schengen States leads to the processing of personal data. At the same time, this inspection helped the national data protection authorities to determine how their country was using Article 99 alerts, which will no doubt have a positive effect on the future activities of those authorities.

In view of the findings of Article 99 inspection, the Joint Supervisory Authority adopted a number of recommendations. The main recommendations were as follows:

- authorities responsible for Article 99 alerts should develop formal and written structured procedures to ensure that Article 99 data were accurate, up to date and lawful;
- there was a need for a clear definition of the types of crimes that could lead to an Article 99 alert. Although the new legal basis for SIS II contained the general term "serious criminal offences ", it was suggested that there should be agreement at European level on 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 could be used for this purpose;

- the appropriate national authorities responsible for Article 99 alerts should control and inspect those alerts every six months. Additional guidelines should be set out;
- the list of authorities (including national security services) that have access to Article 99 alerts should be harmonised in all EU Member States;
- where different authorities were responsible for the quality and integrity of data it should be ensured that these different responsibilities were organised and interlinked in such a way that data were kept accurate, up-to-date and lawful, and that the control of these data was guaranteed;
- an alert concerning contact persons was not permissible in view of the wording of Article 99(2);
- national data protection authorities should inspect Article 99 alerts periodically.

3.2 Article 111 survey

In October 2006, the Schengen Joint Supervisory Authority asked the national data protection authorities to provide information on the implementation and use of Article 111 of the Schengen Convention. This was the third survey initiated on the use of a specific Article of the Schengen Convention (*e.g. concerning Article 96 in the year 2005, Article 99 currently under evaluation*). The need for this survey was established during the examination of a specific case concerning the practical implications of Article 111, which was brought to the attention of the Joint Supervisory Authority.

The Schengen Convention regulates both the rules governing the processing of personal data and the rights of individuals whose personal data are processed in the Schengen Information System. Article 109 of the Schengen Convention determines that the right to have access to data entered in the system should be exercised in accordance with the law of the Contracting Party to the Schengen Convention in which a person invokes that right. It needs to be noted that according to this provision, national law may specify whether the national supervisory authority provided for in Article 114(1) of the Convention should decide whether information should be communicated to the individual involved and by what procedures. Article 109 also governs the situation whereby a natural person intends to exercise the right of access in a State that is a member of the Schengen Convention which did not enter the alert. In such a case, the Schengen State that has not entered the alert may communicate the data only if it has previously given the Schengen State issuing the alert an opportunity to state its position. Article 114(2) gives the individual the right to ask the supervisory authorities referred to in Article 114(1) of the Schengen Convention to check the data concerning him or her that are included in the Schengen Information System, and the use made of such data. As already referred to, this right is governed by the national law of the Schengen State to which the request is made. If the data were included by another Schengen State, the check should be carried out in close cooperation with that State's supervisory authority.

According to Article 109(2) of the Schengen Convention, the right of access is not an absolute right and consequently an individual requesting access to his/her data kept in the Schengen Information System should be refused the communication of data if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third

parties. Moreover, according to Article 109(2) it is forbidden to communicate any data entered in the system for the purposes of discreet surveillance carried out on the basis of Article 99 of the Convention.

Article 106(1) introduces the "owner principle" in the Schengen Information System. Although personal data connected to the alerts are processed in all Schengen States, this does not mean that any Schengen State can change data entered in the system by another State. Although the national law of the processing State applies, the specific provision in the Convention only allows changing or deletion of the data by the State that issued the alert.

Article 111 further guarantees the rights of individuals. Pursuant to Article 111(1) any person may, in the territory of each Contracting Party to the Schengen Convention, bring before the courts or the authority competent under national law an action to correct, delete or provide information or obtain compensation in connection with a report concerning him or her. According to paragraph 2 of this Article, Contracting Parties to the Schengen Convention should undertake amongst themselves to execute final decisions taken by the courts or authorities referred to in paragraph 1.

Following the "owner principle" and the obligation to execute the final decision referred to in Article 111(2), the execution of these final decisions is done by the Schengen State that entered the alert.

In addition, parties to the Schengen Convention are responsible, in accordance with their national law, for any injury caused to a person through the use of the national data file of the Schengen Information System. The quoted provision of Article 116 of the Convention is also applicable to the injuries caused by the reporting party if the data were legally or factually inaccurate.

The objective of the survey was to check whether Article 111 was consistently applied in all Schengen States, respecting the rights of individuals and providing them with fair and equal treatment.

The overview of the courts or competent authorities demonstrated that in the Schengen area a variety of authorities would be competent to deal with Article 111 decisions. In only one State was the Data Protection Authority competent to give a final decision (Austria). In other Schengen States, it was a combination of national data protection authorities and courts or the competence of a specific court.

Regarding alerts from another Schengen State, most answers indicated that there was a formal procedure to consult the alerting state or to involve them officially in the proceedings. However, this was not the case in all Schengen States; at least, it was not mandatory.

As to the involvement of the national data protection authorities in a procedure before the court, the results showed that not all national data protection authorities were formally involved or informed.

Seventeen cases were reported in which Article 111 was applicable.
As to the execution of the decision, no specific procedures to check the execution of a final decision were reported except from Portugal. In general it is the data subject that has to check whether the execution of the decision has taken place.

The joint effort of the national data protection authorities, to survey the national practice followed under Article 111 of the SIS Convention in a certain period and using the same model, once more emphasised a joint concern for the proper use of the SIS. This third joint action emphasised the need for close cooperation between national data protection authorities in the Schengen Area and underlined the need to further invest in cooperation between Schengen States when this is vital to protect the rights of individuals.

Article 111 of the Schengen Convention introduces an important step in safeguarding a subject's right to the correction, deletion, or obtaining of information about him/her entered in the SIS, by introducing the possibility of bringing an action before a court or national competent authority of any Schengen State. This survey demonstrated that this provision is implemented with some variations due to national laws.

A very important cornerstone in safeguarding data subjects' rights is the enforcement of final decisions by the Schengen State issuing the alert. The system of executing any final decision and how this will be applied in practice is of great importance. Although the available statistics are minimal, analysing the cases presented and in particular the cases brought to the attention of the Joint Supervisory Authority, there is sufficient reason to doubt whether Article 111(2) functions in practice.

None of the participating Schengen States reported a follow-up procedure for the execution of a final decision. In most cases, the competent authorities were not involved in the enforcement of their final decisions. This can be due to the national legal framework which differs between the

Schengen States. However, the fact that the enforcement of a final decision by the Schengen State entering the alert was in practice left to the data subject's own initiative is too much of a burden for the data subject.

In view of the findings of the Article 111 inspection, the Joint Supervisory Authority made the following recommendations:

- the Schengen States should evaluate their national proceedings to check whether the safeguards provided for by Article 111 were met;
- Article 111 final decisions must be equally enforced by all Schengen States;
- final decisions that have been taken by courts under Article 111 must be communicated to the national data protection authorities. National regulations may be needed to enforce this need;
- a national procedure for the follow-up of the execution of final decisions taken under Article 111 was necessary in all Schengen States. To this end, communication among the corresponding data protection authorities was necessary. An individual must not be responsible for controlling the execution of decisions relating to him/her in another Schengen State;
- the national data protection authorities should cooperate to this end. The existing principles concerning cooperation between national supervisory authorities must be updated.

3.3 Follow-up of Article 96 inspection

One of the important aspects of supervisory activities is to do periodical follow-up work, to ensure that recommendations which have been made are implemented in practice in the body under supervision, so as to achieve better compliance.

On the initiative of the Joint Supervisory Authority, the national data protection authorities of all Schengen States inspected the use of Article 96 alerts in the Schengen Information System in 2004-2005.

As an alert for refusal of entry might have serious consequences for an individual, and in view of the problems detected in the inspections, the Joint Supervisory Authority agreed on a follow-up check on what had been done at national level with the findings of the report and what improvements have been achieved.

The follow-up check showed that the following steps had been taken at national level in response to the findings of the report: apart from the fact that in some Member States no problems were detected, in other countries very successful follow-up measures were taken. Internal guidelines had been created concerning case-handling and control procedures for the processing of cases that had to be reported under Article 96 of the Schengen Convention, and special attention had been paid to the implementation of one of the recommendations made in the Article 96 report – *measures should be implemented or further developed to prevent Article 96 alerts on nationals from EU Member States*. After the follow-up checks, no alerts on EU Member State nationals were found. The very positive outcome of this follow-up activity was the active awareness-raising campaign undertaken by a number of Member States informing individuals about their rights as stipulated in the Schengen Convention.

Once again this proved the importance of the work done by the Joint Supervisory Authority together with the national data protection authorities, showing their commitment to their values as the protectors of the individuals' rights and freedoms.

The future provisions on alerts on unwanted third state nationals stipulated in the SIS II legal framework will require more individual assessment and responsibility before an alert is entered.

Article 24(1) of 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)[1] provides the criteria for entering an alert in SIS II: data on third-country nationals in respect of whom an alert has been issued for the purposes of refusing entry or stay shall be entered on the basis of a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law taken on the basis of a *comprehensive individual assessment*. This means that the decision to enter the alert cannot be entered automatically into the system. The European Court of Justice, in its judgment on 31 January 2006 (*Commission of the European Communities v Kingdom of Spain*) emphasising the need for the case-by-case evaluation of each individual case, held *that a Contracting State may issue an alert for a national of a third country who is the spouse of a Member State national only after establishing that the presence of that person constitutes a genuine, present and sufficiently serious threat affecting one of the fundamental interests of the society* (…).[2] The Court held that the refusal to grant a visa must be based not on the mere existence of an entry in the SIS or a previous conviction. The Court found that *the existence of a previous criminal conviction can, therefore, only be taken into account in so far as the circumstances which gave rise to that conviction are evidence of personal conduct constituting a present threat to the requirements of public policy*.[3] This Court decision and the provisions of the SIS II legal framework give much more responsibility to the national authorities, when taking decisions which may result in negative consequences for individuals, to comply with international data protection principles right from the start at national level.

Another important change established in Article 42 of the Regulation is the right of third-country nationals who are the subject of an alert issued in accordance with the Regulation to be informed in accordance with Articles 10 and 11 of Directive 95/46/EC. This is an important improvement in comparison with the current situation established by the Schengen Convention.

At the same time, new EU initiatives involving the processing of the personal data of third country nationals give rise to some concern regarding their impact on the rights to privacy of the individuals concerned. According to the European Commission, the Union's common policy in support of Member States' efforts should be continuously developed and strengthened in response to new threats, shifts in migratory pressure and any shortcomings identified, using new technology

[1] OJ L 381, 28.12.2006, p. 4.
[2] OJ C 86, 8.4.2006, p. 3.
[3] OJ C 86, 8.4.2006, p. 3.

extensively and proportionately.[1] According to the Commission, the Union could consider the introduction of an efficient tool for identifying overstayers, as the dates of movements of third-country nationals across the external borders are currently not recorded. Data on third-country nationals (refusals of entry) are currently processed under Article 96 alerts, although without processing the duration of the period overstayed. As this seems not to be sufficient, possible tools are suggested which would apply with regard to third-country nationals travelling to a Member State taking part in Schengen cooperation or to a country associated with such cooperation, and could include:

- facilitation of border crossing for bona fide travellers;
- possible introduction of registration of entry/exit; and
- examining the introduction of an Electronic System of Travel Authorisation (ESTA).

Although this is still at a preliminary stage, the Council conclusions on the development of the VIS[2] welcomed the feasibility study as presented by the Commission, confirming the objectives for a Visa Information System as set out in the guidelines, and invited the Commission to continue its preparatory work on the development of the VIS, in cooperation with Member States, on the basis of a centralised architecture taking into account the option of a common technical platform with SIS II, storing the data on the same system and accessed by the same end-users. This might mean that if both systems were created on a common technical platform, technical measures/facilities for interoperability between SIS II and the VIS would be possible. Although it is not yet proved that this new system will provide added value for the external borders of the EU in comparison with the existing EU systems (SIS), it is clear that this larger scale, complex and interlinked model of data processing will have a serious impact on the privacy of individuals and will require huge efforts from national and European data protection authorities to ensure the proper and effective protection of individuals' rights. The price of these initiatives could be described like this: "To modernise immigration policy at the cost of dehumanising it is the effect of an asymmetry in policy development where control of migrants is extended without a corresponding development of their rights".[3]

[1] COM(2008) 69 final, 13.2.2008.
[2] 6535/04, 20 February 2004.
[3] Alice Garside (2006), The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?, Sussex Migration Working Paper no. 30.

4. OPINIONS OF THE JOINT SUPERVISORY AUTHORITY

4.1 Interpretation of Article 111 of the Schengen Convention

In June 2006 the Joint Supervisory Authority received a request from the Austrian data protection authority to examine any difficulties concerning the implementation of Article 111 of the Schengen Convention in accordance with Article 115(3) of the Schengen Convention, and to draw up proposals for any problems which may exist. In view of the circumstances leading to the request, the Joint Supervisory Authority also examined the impact of coinciding procedures on the implementation of Article 111.

With the creation of the Schengen Information System, specific alerts on individuals are exchanged between the States that are party to the Convention. The Convention defines the reasons and conditions for these alerts as well as the actions to be taken. One of the most important achievements of the Convention is probably the obligation on the States participating in the Schengen Information System to act (directly) on an alert from another State.

The relation between the national law of the Schengen States and the Convention is clearly defined in Article 104(2): "*In so far this Convention does not lay down specific provisions the law of each Contracting Party shall apply to data entered in its national section of the SIS*".
This indicates that specific provisions in the Convention prevail in situations where national laws contain different provisions.

An example of such a specific provision is the so-called "owner principle" in Article 106(1): "*Only the Contracting Party issuing the alert shall be authorized to modify, add to, correct or delete data which it has entered".*
Although personal data connected to the alerts are processed in all Schengen States, this does not mean that the processing State can change data entered in the system by another State. Although the national law of the processing State applies, the specific provision in the Convention only allows the changing or deletion of the data by the State that issued the alert.

The harmonisation achieved in creating the Schengen Information System included the position of data subjects. Data subjects' rights were specified, including provisions preventing data subjects being faced with procedural "hindrances" in pursuing their rights. The mere fact that the subject

may not be in a position to travel to the Schengen area should not cause any obstacle to requesting any legal action.
Recognising their position, the Convention does not oblige the data subject to start (legal) proceedings regarding an alert in the State that issued the alert. It is left up to the data subject to start such a procedure in any of the Schengen States of his choice. By doing so, the Schengen States made a clear statement of trust in a harmonised implementation of the applicable data protection rules.

The rights of the data subject are defined in Article 109(1) - the right to have access - and in Article 110 - the right to have factually inaccurate data corrected or unlawfully stored data deleted.
These rights are to be exercised in accordance with the law of the Schengen State before which these rights are invoked (Article 109(1)). If data are entered in the Schengen Information System by another Schengen State, that State shall be given the opportunity to state its position before a decision is made.

Furthermore, the data subject has the right to ask a national data protection supervisor of a Schengen State to check his data (Article 114(2)). If those data were entered in the Schengen Information System by another State, the national supervisor is to coordinate this check with the national supervisor in the Schengen State responsible for the alert.

The data subject is also given the right, before a court or an authority competent under national law, to bring an action to correct, delete, to obtain information or compensation in connection with an alert involving the data subject (Article 111(1)).
The second paragraph of Article 111 obliges the Schengen States to mutually enforce final decisions as referred to in Article 111(1).
In view of the system of guaranteeing the rights of the data subject in the Convention and especially the existence of the "owner principle", a mechanism is required to ensure that final decisions of courts or authorities as referred to in Article 111(1) are enforced, even by other Schengen States. Without such a mechanism, the principal data protection rights granted to a data subject in the Schengen Convention are not sufficiently safeguarded.

One of the conditions for the entry into force of the Convention is that the participating State has adopted the necessary national provisions in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of

28 January 1981 and in accordance with 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.

All Schengen States have implemented the necessary data protection legislation, but the way it is implemented may demonstrate some differences. There are States in which the rights of the data subject are primarily dealt with in direct contact between the data subject and the authority responsible for the national part of the Schengen Information System. In other States, the national supervisors fulfil an important role as intermediary between that authority and the data subject.

The Schengen Convention recognises these differences in some of the specific provisions concerning the data subject's rights (e.g. Article 109). However, where no provision is laid down for combining the Schengen and national provisions, the Schengen provision providing for a specific rule applies (Article 104(2)).

This will be the case where an action as referred to in Article 111(1) is brought before a national court or competent authority of a State other than that responsible for the alert and where at the same time this alert is also subject of a legal procedure in the State responsible for the alert. Article 111 does not contain a provision regulating this situation. Taking into account the specific and fundamental nature of Article 111, the conclusion is justified that in the situation as described, Article 111 prevails.

In practice this should not cause problems since all Schengen States recognise in their national procedures the principle of hearing all parties involved. A procedure as referred to in Article 111 should in practice not lead to a final decision without hearing the State responsible for the alert. The existence of another legal procedure will no doubt be taken into account by the court or authority as referred to in Article 111.

Where this information has not been made available, or when available has not led to another decision, the specific character of Article 111 forces Schengen States to enforce that final decision.

It should furthermore be noted that if such a decision leads to the deletion of the Schengen alert, it is left up to the alerting State to introduce a national alert into its national systems. A similarity can be found with Article 25 of the Schengen Convention: if a residence permit is issued by a Schengen State to an alien on whom an alert has been issued for the purposes of refusing entry, the state issuing the alert should withdraw the alert but may put the alien concerned on its national list of alerts.

Although Article 111 of the Schengen Convention does not provide for the clear definition on the "final decision", some authors are of the opinion that "*"final decisions" should not be interpreted too narrowly. It does not imply that this only covers decisions of the highest (administrative, civil or criminal) courts. The fact that Article 111 CISA and Article 43 of the SIS II Regulation also refers to decisions of national data protection authorities, means that a decision should be considered as final, as long as the decision is executable and none of the parties lodged an appeal against this decision*"[1].

Despite possible different interpretations of the term "final decision" depending on the differences in legal systems and procedures, the Joint Supervisory Authority in its opinion concluded that any final decision of a court or authority as referred to in Article 111 and dealing with an alert entered by another Contracting Party should always be enforced by that other party.

Considering the judgment of the Court of Justice (*Commission of the European Communities v Kingdom of Spain*)[2] and drawing a parallel between the obligation of the Schengen States to accept and enforce the decision taken by another Schengen State to refuse entry or a visa and the obligation and acceptance of the final decision of a court or authority to delete an alert from the SIS, practice shows some failures to enforce decisions of national courts or authorities to delete alerts, which results in negative consequences for the individual concerned.

[1] Evelien Brouwer, "The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts", CEPS Working Document No. 288/April 2008.
[2] OJ C 86, 8.4.2006, p. 3.

4.2 Opinions on the implementation of Article 102A (SCHAC 2501/07)/ SCHAC 2504/08

According to Article 102A(4), the Council must submit a report on the implementation of Article 102 A of the Schengen Convention, and more specifically on the applicable data protection rules, to the European Parliament after seeking the opinion of the Joint Supervisory Authority.

Following the request of the Chairman of the SIS/SIRENE Working Party on 31 May 2007, the Joint Supervisory Authority adopted an opinion in June 2007.
Article 102A of the Schengen Convention introduces, for services in the Member States responsible for issuing registration certificates for vehicles, a right to have access to specific data in the Schengen Information System. This concerns data on motor vehicles, trailers and caravans which have been stolen, misappropriated or lost, and registration certificates for vehicles and number plates.
Pursuant to decision 2006/228/JHA, data on these certificates and number plates may be processed in the Schengen Information System since 31 March 2006.

The report clearly showed that the general implementation of Article 102A was not yet complete in all the Member States. In view of this, the opinion focused on some specific data protection elements relating to implementation.
In view of the lack of clear and visible results in the first year, the Joint Supervisory Authority could only conclude that the control on the use of data on objects as provided for in Article 102A was not in compliance with Article 103, and that the Council should further explore whether the Member States were fulfilling their obligations under Article 103 in relation to Article 102A.

Since a strict implementation of Article 103 was not only of importance for access by vehicle certification services, the Joint Supervisory Authority indicated that it should request the national data protection authorities to report on the way Article 103 was implemented in their States.

The draft report contained the remark that registration certificates for vehicles and number plates were not personal data. The Joint Supervisory Authority stressed that this remark and the context in which it was made was not in line with what is considered as personal data. The general definition of personal data as used in all relevant data protection legal instruments, describes personal data as "*any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly*".

The Joint Supervisory Authority noted that national data protection authorities generally considered registration certificates and number plates as personal data, unless the circumstances of processing did not give any possibility for identification of the holder of the certificate or number plate.

The Joint Supervisory Authority furthermore noted with some concern that in some countries the checks as laid down in Article 102A were already performed before the implementation of this Article. The only conclusion that could then be drawn was that these activities must be considered as a misuse under the national law of those countries. This conclusion strengthened the Joint Supervisory Authority's policy to continuously stimulate the development of control mechanisms including periodic inspections of the use of the Schengen Information System.
In conclusion, the Joint Supervisory Authority, acknowledging that the implementation of Article 102A and the processing of registration certificates and vehicle number plates by all Member States were not yet completed, indicated that it had its concerns on this implementation. These concerns specifically related to the apparent lack of control on use. The Joint Supervisory Authority urged the Council to take care that Member States fulfilled their obligations under Article 103 in relation to Article 102A.

The Joint Supervisory Authority asked for this opinion to be attached to the report to the European Parliament.

On 7 July 2008, the Joint Supervisory Authority received a request from the SIS/SIRENE Working Party to give an opinion on the implementation of Article 102 A during 2007.

In its opinion the Joint Supervisory Authority noticed that the implementation of the CISA in nine new Schengen States on 1 September 2007 was not taken into account. According to Annex I to the Council Decision 2007/471/EC, the provisions of Article 64 and Articles 92 to 119 of the CISA, as well as Regulation (EC) No 1160/2005, were applicable to the new Schengen States from 1 September 2007. Although these new States may not have actually implemented Article 102A, the report did not present any information on this.

Once again the Joint Supervisory Authority emphasised that a proper logging of the use by vehicle registration offices of certain data to establish whether a vehicle was stolen, misappropriated or lost was necessary. As the report provided a similar overview as in 2006, the Joint Supervisory Authority repeated its conclusion from 2006 *"that the control on the use of data on objects as provided for in Article 102A, is still not in compliance with Article 103"*. The Joint Supervisory

Authority also issued a reminder about the position taken by national data protection authorities as to whether data entered into the SIS in accordance with Article 102A were considered personal data and the Member States' obligations in relation to the proper implementation of Article 103 in relation to Article 102A.

4.3 Opinion on the implementation of a mail server relaying SIRENE messages in a central point in C.SIS premises (SCHAC 2502/07)

The Joint Supervisory Authority received a request from the Chairman of the Article 36 Committee for an opinion concerning the implementing of a centralised star-topology architecture for the exchange of SIRENE messages and the proposed principles for communication between countries. In its opinion the Joint Supervisory Authority focused on the principles for communication as described in the request as well as on some principles concerning the availability of the network.
In this respect, the Joint Supervisory Authority stressed that the technical support function of the Schengen Information System, as well as the proposed use of a mail server at C.SIS, should comply with the data protection principles set out in the Schengen Convention, together with the principles of the Council of Europe Convention of 28 January 1981 and of Recommendation No R(87)15 of the Committee of Ministers of the Council of Europe. In view of this, the following quality requirements should be met:

i) Confidentiality: ensuring that information was accessible only to those authorised to have access, and
ii) Availability: ensuring that authorised users had access to information and associated assets when required.

Describing the implementation of the confidentiality principle in the use of the mail server at C.SIS and the procedures as described in the request, the Joint Supervisory Authority noted that this should lead to the following measures:

1. Stored messages should be always kept encrypted during the storage period.
2. Messages that were sent by C.SIS to the recipient must be deleted directly after the receipt of the delivery report.
3. Messages which failed to be delivered to the recipient (after a certain number of trials) should in principle be sent back to the sender accompanied by a delivery failure status report.

4. The request did not mention which encryption key to be used by the SIRENE bureaux for the delivery of the messages if the backup server in Austria was activated (due to a C.SIS server failure).

   a) If the private key of C.SIS is also used in the back-up facility, this key was under severe risk since it is a standing principle that a private key should never be known to anyone other than the owner of the key; or

   b) A separate Austrian key is used. In this case, a formal procedure should be in place describing the tasks involved in managing inconsistencies deriving from the use of different public keys to deliver messages from national bureaux to the server. In addition, the transition procedure of the messages, encrypted with the backup server's public key, to the C.SIS server (and vice versa) should be described. Finally, a backwards resolution procedure concerning messages encrypted with keys which were no longer valid should also be described.
5. A key management procedure should be described.
6. A procedure for handling messages marked to be of non-use (for any reason) should be described.

The implementation of the availability principle in the use of the mail server at C.SIS should lead to the following measures:

1. To increase the availability of the mail delivery subsystem, the communication line for mail server messages should be different from the line between N.SIS and C.SIS.
2. The C.SIS mail server should also have an alternate line for routing messages if the main routing line was unavailable.
3. A short Risk Analysis was recommended for availability matters (response times, time needed for back up, what if scenarios etc.). A Business Continuity Plan would also be recommended for this specific procedure.

4.4 Opinion on the draft implementing measures including the SIRENE Manual for the second generation Schengen Information System (SCHAC 2503/07)

Following the Commission's request for an opinion on the draft implementation measures including a revised SIRENE Manual for the second generation Schengen Information System, the Joint Supervisory Authority adopted an opinion in October 2007.

In its opinion the Joint Supervisory Authority paid special attention to the conservation periods for logs, wondering why the longest period of retention was chosen instead of a period of one year as indicated in Article 18(3) of the Council Decision of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System [1] and Article 18(3) of the Regulation of the European Parliament and of the Council dealing with the same subject [2].

Another concern touched upon by the Joint Supervisory Body was the deletion of expired European Arrest Warrants (EAW). The Joint Supervisory Authority noticed that an EAW that had expired was not deleted automatically, but had to be deleted by the Member State. At the same time the Member State would check whether it had also entered other EAWs concerning the same person which might lead to an extension of the alert. Experiences with such deletion procedures were not all positive and it was therefore recommended that the expired records should be automatically deleted. The Joint Supervisory Authority recommended the implementation of a technical solution, to only delete the EAW and not the alert, in case more EAWs existed concerning the same person.

In its opinion the Joint Supervisory Authority also focused on the format and quality of biometric data. It called for attention to be paid to the wider use of fingerprints than photographs as allowed according to the Council Decision. Such biometric data should only be used to confirm the identity of a person who had been located as a result of an alphanumeric search made in SIS II.

Analysing the possible effects on data protection principles while linking alerts, the Joint Supervisory Authority suggested that it should be ensured that the provisions in the text were amended so as to underline that access rights were decisive in allowing access to linked alerts.

Referring to the possible types of searches in the SIS II, the Joint Supervisory Authority stressed that in view of the purpose of the SIS II, the standard query should be made compulsory leaving the possibility for other search queries according to need, in relation to the results of the first standard query. The Joint Supervisory Authority strongly suggested amending the text to make clear that the standard search was always the compulsory first search to be made in the SIS II followed when necessary by another search.

Another aspect that needed attention was the definition of the "extended query" as a feature designed to perform complex queries that were not covered by other types of queries and which

[1] OJ L 205, 7.8.2007, p. 63.
[2] OJ L 381, 28.12.2006, p. 4.

could be defined by users using a special query language. The Joint Supervisory Authority strongly suggested reconsidering this "extended query" and defining which search criteria may be used within the framework of the Council Decision and the Regulation.

The Joint Supervisory Authority also presented its remarks on the revised SIRENE Manual. The Authority concentrated on the use of SIS II for other purposes and wondered how the SIRENE bureau of the Member State entering the data could fulfil its obligations to coordinate the verification of the quality of the information as defined in Article 7(2) of the Council Decision and of the Regulation. The Joint Supervisory Authority also reflected on the different responsibilities for the quality of the data and the need for specific rules on how these responsibilities should be implemented and verified.

Another concern raised by the Joint Supervisory Authority was the input mask containing 15 categories of information related to fingerprints and the relevance of the additional information, and the compliance of such processing with the Council Decision and the Regulation.

An important element of this opinion was the relationship between SIRENE and Europol. The Joint Supervisory Authority strongly supported such cooperation when this contributed to the quality of the data processed in SIS II or when it contributed to creating compliance with specific articles in the Council Decision concerning Europol's access to SIS II.
Article 41(2) of the Council Decision obliges Europol to inform a Member State when a search reveals the existence of an alert in SIS II. Chapter 2.14 of the Manual refers to the Europol National Unit of the Members States' point of contact. It should however be noted that since the recent amendment [1] to the Europol Convention it will be possible for this unit no longer to be the only liaison bureau between Europol and a Member State (see Article 4(2) of the Europol Convention). Furthermore, and in view of Europol's tasks, the reason for informing a Member State via the Europol National Unit might be diverse in nature and also in level of confidentiality. A strict obligation to inform SIRENE about any exchange as proposed in the Manual may not be in compliance with specific conditions applicable to the exchange between Europol and its contact points in the Member States. The Joint Supervisory Authority suggested reformulating Chapter 2.14 and, with reference to Member States' responsibility for the quality of data, introducing an obligation that information becoming available through contacts between Europol and the Member States which might lead to a change or deletion of the SIS II alert must be communicated to the SIRENE bureau.

[1] OJ C 2, 6.1.2004, p. 3.

4.5 Opinion on the principles governing cooperation between national supervisory authorities based on the Schengen Convention

In November 1996, the Joint Supervisory Authority decided to set up principles governing cooperation between national supervisory authorities. Based on experiences with this cooperation and a survey of the Joint Supervisory Authority into the implementation of Article 111, it was decided to update the 1996 principles. Therefore the Joint Supervisory Authority adopted a new opinion on the principles governing cooperation between national supervisory authorities based on the Schengen Convention in June 2008.

The enhanced exchange of law enforcement information throughout the EU, creating a situation in which data relating to one person may be processed in different Member States and/or EU organisations, did not make it easy for a data subject to avail himself of his rights.
Different national laws and procedures as well as the existing language barriers only added more obstacles for the data subject.

Examples of specific cooperation between national data protection authorities in relation to data subject's rights can be found in the Schengen Convention. A data subject may ask for access in any of the Schengen States, also in a situation where that Schengen State is not responsible for entering the data in the Schengen Information System (SIS). Specific rules on the applicable law and mutual cooperation between national data protection authorities are defined. Although the term "close coordination" is not defined in the Schengen Convention, the data protection authorities have an obligation to cooperate in such a way as to fully assist each other and the individual exercising his rights.

What does that mean in practice? It means that the exercise of the data subject's right should guarantee for an individual an access to justice which is a part of effective legal protection.
The importance of the Convention is the recognition that data subjects will not always be able to go to another State or to approach an authority in that State in order to invoke their rights, for example in view of the travel costs or language barrier. In this respect experiences with the SIS and data subject's rights provide us with information on how cooperation between national data protection authorities could be further developed.

The basic principles are based on the following Articles[1]:

Article 106(3) describing the procedure if Schengen States cannot come to an agreement on whether data are factually incorrect or unlawfully stored;

Article 109 describing the right of access and the procedure to be followed;

Article 110 describing the right any person has to have factually incorrect data corrected or unlawfully processed data deleted;

Article 111 describing the right to address a court and the undertaking of Schengen States to enforce final decisions of courts;

Article 114 describing the right to ask a national supervisory authority to check data and the procedure to be followed if those data were entered by another Schengen State.

The Joint Supervisory Authority considered several practical issues in its opinion.

Language: The present practice in cooperation demonstrated that sometimes requests or answers to requests were provided in the language of the requesting and requested authority. Since the documents prepared by the national supervisory authorities may also need to be presented to the data subject, a situation might arise that a data subject received information in another language.

Two scenarios were possible:

- All correspondence takes place in one language in which case the English language is suggested.
- All correspondence takes place in the languages of the parties involved, each taking responsibility for a formal translation comprehensible to the other national supervisory authority and the data subject.

Time limits: In view of the interests at stake for the data subject, requests for cooperation will be dealt without undue delay.

Contact persons: In order to further facilitate cooperation, there will be a list of contact persons in each of the national supervisory authorities. In view of the difficulty of having such a list continuously updated, the members of the Joint Supervisory Authority will be the contact persons.

4.6 Opinion on the Schengen Information System and violent troublemakers 08/10

In the summer of 2008, the Joint Supervisory Authority took note of the discussions in the SIS/SIRENE Working Party on the use of Article 99 alerts in the Schengen Information System for

[1] The new legal basis for SIS II contains similar provisions with the exception of Article 114.

violent troublemakers. These discussions concentrated on the inclusion of new categories of data in the SIS: data on violent troublemakers which concerned persons to be barred from certain events, such as European summits or similar venues, international sports or cultural events or other mass gatherings using Article 99 alerts under the Schengen Convention.

This proposal raised a number of questions from the data protection point of view. The Joint Supervisory Authority sent a letter to the Chairman of the SIS/SIRENE Working Party/Mixed Committee expressing its concern and doubts regarding this initiative. The Joint Supervisory Authority also regretted that it was not consulted on this issue at an earlier stage.

First of all, the Joint Supervisory Authority noted that an Article 99 alert was specifically related to the prosecution of a criminal offence which had already been initiated or to the prevention of threats to public security. This was the prerequisite for Article 99 alerts. In view of the proposed purpose for the use of Article 99 SIS, one may assume that the prevention of threats to public security was the only aim of the (proposed) alert. Furthermore, an Article 99 alert may only be entered in the SIS regarding a person who intended to commit or was committing numerous and **extremely serious criminal offences** or if there was an overall assessment for this person based on information concerning past criminal offences giving reason to believe that the person would commit **extremely serious criminal offences** in the future. The term "**extremely serious criminal offence**" is not defined in the Convention and criminal laws may differ from country to country. In view of the description of this group as "violent troublemakers" and related to mass gatherings as international sports, cultural events and European summits or similar events (G8), the Authority raised doubts as to whether the kind of activities described in the proposal could be classified as "**extremely serious criminal offences**" and lead to an alert under Article 99. The Joint Supervisory Authority also pointed out that the term "troublemaker" was not defined either in the Schengen Convention or in any European or international legal instrument. Since there was no clear definition and harmonised interpretation of this term, there was a great risk that data on innocent persons would be entered in the SIS without any justification. The purpose of alerts on these persons was to bar them from events. Barring would mean not allowing them to be in the vicinity of such events or even not to allow them in the country where the event was taking place. In this respect, the Joint Supervisory Authority noted that Article 99 of the Schengen Convention did not provide for coercive measures (arrest cannot be carried out under this Article) and that it could be used only for the purposes of discreet surveillance or specific checks. Therefore, the purpose of the proposal in itself was not clear and would no doubt lead to deviation from the original purpose of Article 99 alerts.

The Schengen Convention as well as the new legal basis for SIS II [1] clearly limited the use of these alerts to a specific category of persons and a specific category of crime. The category of crime is described in the Schengen Convention as "extremely serious criminal offences" and in the Council Decision as "serious criminal offences" with a clear reference to the offences summed up in Article 2 of the Council Framework Decision on the European arrest warrant and the surrender procedures between Member States. The only crime mentioned in that Framework Decision that related to violence that might take place in relation to the events from which people should be barred is murder or grievous bodily injury.

Another aspect that was emphasised was the purpose of the alert and the expected action to be taken. Article 99 of the Schengen Convention and Article 36 of the Council Decision describe the purpose of the alert as discreet surveillance or a specific check (Schengen Convention) or discreet checks or specific checks (Council Decision).

Also, the Article 99 survey by the Joint Supervisory Authority clearly demonstrated that the national law of certain Schengen States did not allow the possibility for the competent authorities to carry out specific checks, while in some States a court order was required.[2]

In view of the proposed use of these alerts to bar violent troublemakers from certain events which might include arrest and detention, the Joint Supervisory Authority concluded that this use of Article 99 would be in breach of the purpose as defined in the Schengen Convention and the Council Decision. This, and the conclusion that there was apparently no realistic relation between violent troublemakers and the category of persons defined in the Schengen Convention and the Council Decision made the proposed use not in compliance with the legal basis and thus illegal.

[1] Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II).
[2] Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System, SCHAC 2501/08, Brussels, 18 January 2008.

5. DATA SUBJECTS' RIGHTS

In defining the rights of data subjects, the Schengen Convention provides for a system for data subjects to implement their rights in any Schengen State.

According to Article 115(3) of the Schengen Convention, the Joint Supervisory Authority shall also be responsible for examining any difficulties of application or interpretation that may arise during the operation of the Schengen Information System, for studying 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 for drawing up harmonised proposals for joint solutions to existing problems.

It should be emphasised that Title IV, Chapter 3, of the Schengen Convention deals with the protection of personal data and security of data in the Schengen Information System. The obligations of the States participating in the SIS and the rights of the data subject are described in that chapter. Article 115 introduces the Joint Supervisory Authority and describes the tasks and competences of that authority. This Article does not give the Joint Supervisory Authority competence or powers to intervene in conflicts between States in individual cases.

However, if a case comes to the attention of the Joint Supervisory Authority in which the interpretation of the Schengen Convention needs clarification or a harmonised proposal, the Authority is competent to deliver an opinion.

On 17 August 2005, the Joint Supervisory Authority received a request from the legal representative of Mr X, a third-country national. The Joint Supervisory Authority was asked to do what was within its powers concerning a French Article 96 alert, and a decision of the Austrian Data Protection Authority ordering the deletion of that alert. The Article 96 alert had been entered by France denying Mr X access to Schengen territory; based on that alert, the Austrian authorities refused Mr X a visa. The representative requested access to the data processed and was informed by the Austrian Ministry of Home Affairs that an Article 96 alert existed, entered by the French authorities. Mr X's representative started a procedure with the French Data Protection Authority – CNIL – to have the data deleted, via a French lawyer. This procedure did not lead to the deletion of the data. Mr X's representative started a procedure against the French Ministry of Home Affairs with the Austrian Data Protection Commission. By decision of 7 June 2005, the Austrian Data Protection Commission declared the complaint valid and ordered the deletion of the alert within a period of three weeks. The alert should thus have been deleted on 12 July 2005. The French

authorities did not delete the alert. Mr. X's representative requested the Joint Supervisory Authority to act in this case.

In this particular case, the Joint Supervisory Authority noted that there was a coincidence in this case of two different procedures: one in Austria having led to the decision of the Austrian Data Protection Commission and one in France at the Conseil d'Etat related to the refusal of French Ministry of Interior to correct or delete the alert as requested by Mr X. In view of the specific nature of this case, the Joint Supervisory Authority presented its interpretation of Article 111 to all parties.

Looking to the future legal framework of SIS II as regards the rights of data subjects, positive new provisions have been included in this legal framework in comparison with the Schengen Convention. First of all, the right of information for third-country nationals who are the subject of an alert issued in accordance with Regulation (EC) 1987/2006 is provided in Article 42 of the Regulation. Council Decision 2007/533/JHA and Regulation (EC) 1987/2006 put more responsibility on the Schengen States, obliging them (Article 58 and Article 41), in the event of an individual's request for access, correction and deletion of data, to inform the individual as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides. What is important is that both the Council Decision and the Regulation contain the obligation on States to inform individuals about the follow-up given to the exercise of their rights of correction and deletion as soon as possible and in any event not later that three months from the date on which they apply for correction or deletion or sooner if national law so provides. This right is of the utmost importance for the data subject, who can find out promptly what personal data concerning him is being processed in the system.

6. FUTURE OF JOINT SUPERVISION

The application of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (the Council Decision) and 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) (the Regulation), will bring new changes to the future joint supervisory framework for the SIS II. What is also important is that the new coordinated supervision will not lessen the level of supervision laid down by the Schengen Convention. Article 61 of the Council Decision stipulates that the European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with the Decision. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly. Article 62 of the Council Decision creates a new legal framework for coordination between the national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences; they are to cooperate actively in the framework of their responsibilities and ensure coordinated supervision of SIS II. Similar provisions are embodied in the Regulation. The content of future cooperation will be as follows: the national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, are to exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of the Council Decision (the Regulation), study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary. The national supervisory authorities and the European Data Protection Supervisor are to meet for that purpose at least twice a year. Rules of procedure are to be adopted at the first meeting. Further working methods are to be developed jointly as necessary. A joint report on activities is to be sent to the European Parliament, the Council, the Commission and the Management Authority every two years. Therefore the joint supervisory regime and its infrastructure established by Article 115 of the Schengen Convention will change into the new cooperation framework. Worth mentioning is the fact that Article 44 of the Regulation provides that the authority or authorities designated in each Member State and endowed with the powers referred to in Article 28 of Directive 95/46/EC are independently to monitor the lawfulness of the processing of SIS II personal data on their territory and its transmission from that territory, and the exchange and further processing of supplementary information. This means that national data protection authorities will have broader powers in comparison with Article 114 of the

Schengen Convention.

Article 63 of the Council Decision lays down the provisions of data protection during the transitional period, providing that where the Commission delegates its responsibilities during the transitional period to another body or bodies pursuant to Article 15(4), it shall ensure that the European Data Protection Supervisor has the right and is able to fully exercise his tasks, including carrying out on-the-spot checks, and to exercise any other powers conferred on him by Article 47 of Regulation (EC) No 45/2001.

However the question remains as to the guarantees for data protection during the migration phase from SIS I+ to SIS II to the joint supervision regime. What are the most recent challenges for joint supervision? The smooth migration of data from SIS 1+ to SIS II and the smooth transition from the Joint Supervisory Authority to coordinated supervision? On 30 June 2008 the Committee on Civil Liberties, Justice and Home Affairs organised a Round Table on "Liberty and Security in Integrated Management of EU Borders", with one session dedicated to the subject "Data Protection implications of the Migration from SIS I+ to SIS II". The Chair of the Joint Supervisory Authority and the European Data Protection Supervisor were invited to contribute to the discussions, giving their thoughts on this subject. Both expressed the unified position that there would be no overlap of the competencies of the two supervisory bodies. The European Data Protection Supervisor expressed his confidence in the smooth transition in the actual supervision of the system; the migration phase would be the opportunity to initiate this "partnership". Both speakers confirmed their belief in the successful coordinated supervision of the system during the transitional period, in preparation for actual co-supervision of the system.

Looking at the future coordinated supervision framework, it is justified to pay tribute to and acknowledge the importance and influence of the work of the Schengen Joint Supervisory Authority. The years of the strong commitment and hard work, building up experience, knowledge and trust in its competence, will be of fundamental worth to the future work of the national supervisory authorities together with the European Data Protection Supervisor. Of course, the difficulties of supervising such complex data bases as SIS II will require more time and effort in order to demonstrate the effectiveness of such coordinated supervision. It is beyond doubt that in future supervision will continue to work successfully, benefiting from the experience and knowledge built up by the Joint Supervisory Authority.

7. MEMBERS OF THE SCHENGEN JOINT SUPERVISORY AUTHORITY

Chairman: **Mr Georges de La LOYERE**

Vice-Chairman: **Ms Angelika SCHRIEVER-STEINBERG**

AUSTRIA MEMBERS Ms Waltraut KOTSCHY Ms Eva SOUHRADA-KIRCHMAYER ALTERNATE Mr Gregor KONIG	BELGIUM MEMBERS Mr Willem DEBEUCKELAERE Mr Bart DE SCHUTTER ALTERNATE Ms Priscilla de LOCHT
CZECH REPUBLIC MEMBER Ms Ludmila NOVAKOVA ALTERNATE Ms Miroslava MATOUSOVA	DENMARK MEMBERS Ms Lena ANDERSEN Mr Sten HANSEN ALTERNATES Mr Jens Harkov HANSEN Mr Ole TERKELSEN
ESTONIA MEMBER Mr Taago PAHKEL ALTERNATE Ms Kaja PUUSEPP	FINLAND MEMBERS Mr Reijo AARNIO Ms Elisa KUMPULA ALTERNATE Mr Heikki HUHTINIEMI
FRANCE MEMBER Mr Georges de La LOYERE ALTERNATE Mr Michel MAZARS	GERMANY MEMBERS Mr Peter SCHAAR Ms Angelika SCHRIEVER-STEINBERG ALTERNATES Mr Wolfgang Von POMMER ESCHE Mr Michael RONELLENFITSCH
GREECE MEMBER Mr Leonidas KOTSALIS ALTERNATE Ms Maria ALIKAKOU	HUNGARY ALTERNATE Ms Agnes PAJO
ICELAND MEMBERS Mr Bjorn GEIRSSON Ms Sigrun JOHANNESDOTTIR Ms Thordur SVEINSSON	ITALY MEMBERS Mr Giovanni BUTARELLI Ms Vanna PALUMBO

LATVIA MEMBERS Ms Signe PLUMINA Ms Aiga BALODE	LITHUANIA MEMBERS Ms Rita VAITKEVIČIENĖ Ms Neringa KAKTAVIČIŪTĖ-MICKIENĖ
LUXEMBOURG MEMBERS Mr Georges WIVENES Mr Pierre WEIMERSKIRCH ALTERNATE Mr Thierry LALLEMANG	MALTA ALTERNATE Mr David CAUCHI
NETHERLANDS MEMBERS Mr Jacob KOHNSTAMM Ms Jannette BEUVING ALTERNATE Ms Laetitia KRONER	NORWAY MEMBERS Mr George APENES Ms Guro SLETTEMARK ALTERNATE Ms Astrid FLESLAND
POLAND MEMBER Mr Michał SERZYCKI ALTERNATE Mr Piotr DROBEK	PORTUGAL MEMBERS Mr Luis BARROSO Ms Isabel CERQUEIRA DA CRUZ ALTERNATE Ms Clara VIEIRA CARDOSO GUERRA
SLOVAK REPUBLIC MEMBER Mr Peter LIESKOVSKY ALTERNATE Mr Tomaš MIČO	SLOVENIA MEMBERS Ms Alenka JERSE Ms Natasa PIRC MUSAR ALTERNATE Mr Marijan ČONČ
SPAIN MEMBER Mr Rafael GARCIA GOZALO ALTERNATE Ms Marta AGUIRRE CALZADA	SWEDEN MEMBER Ms Elizabeth WALLIN ALTERNATE Ms Birgitta ABJORNSSON
SWITZERLAND MEMBERS Mr Bruno BAERISWYL Mr Jean-Philippe WALTER	

8. OBSERVERS OF THE SCHENGEN JOINT SUPERVISORY AUTHORITY

BULGARIA Mr Veselin TSELKOV Mr Valentin ENEV	CYPRUS Ms Goulla FRANGOU Ms Louiza MARKIDOU
IRELAND Mr Billy HAWKES Ms Anne GARDNER Ms Ann McCABE	LIECHTENSTEIN Mr Philipp MITTELBERGER
ROMANIA Ms Georgeta BASARABESCU Ms Nicoleta RUSU Ms Simona SANDRU Ms Alina SAVOI Mr George GRIGORE	UNITED KINGDOM Mr David SMITH Ms Jane DAWSON