



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 17 January 2011

5183/11

**SIRIS 5
COMIX 13**

COVER NOTE

from: Ms Angelika Schriever-Steinberg, Chair of the Schengen Joint Supervisory Authority

to: Mr Serge Kinet, Chairman of the Working Party for Schengen Matters (SIS/SIRENE)

Subject: 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

Delegations will find in the annex a 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.

Mr Serge Kinet
Chairman of the SIS/SIRENE Working Group
Council of the European Union
175, Rue de la Loi
B-1048 BRUSSELS

Brussels, 13 December 2010

Report of the Schengen Joint Supervisory Authority on the follow-up of recommendations concerning the use of Article 96 alerts in the Schengen Information System

Dear Mr Kinet

In 2005 the Schengen Joint Supervisory Authority reported on its inspection of the use of Article 96 alerts in the Schengen Information System. That report included seven recommendations to improve the implementation of - and ensure compliance with - Article 96 of the Schengen Convention.

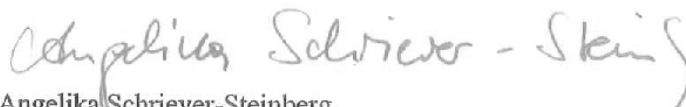
In 2008 the Joint Supervisory Authority asked its members to check what had been done at national level following the publication of the 2005 report. The enclosed report is the product of that follow-up check.

As you will see, the report concludes that while some Schengen Member States have shown improved compliance, others have not. Gaps in compliance have been identified and must be rectified.

It was therefore decided to distribute the report to you and other relevant stakeholders in order to raise awareness of these issues and highlight the areas requiring close attention.

Should you require any further information on this matter, please do not hesitate to contact us.

Yours sincerely



Angelika Schriever-Steinberg
Chair of the Schengen Joint Supervisory Authority

ARTICLE 96

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

Report 10-11Rev.01, Brussels, 26 November 2010

SCHENGEN
Joint Supervisory Authority



Joint Supervisory Authority of Schengen • Autorité Commune de Contrôle de Schengen
Data Protection Secretariat • 175, Rue de la Loi • B-1048 Bruxelles

Content

<i>Content</i>	2
<i>Introduction</i>	3
<i>Recommendations</i>	3
<i>Reactions received</i>	4
<i>Results</i>	5
<i>Schengen Data Protection Catalogue</i>	11
<i>Raising awareness</i>	11
<i>Conclusion</i>	11
<i>ANNEX</i>	12

Introduction

The JSA Schengen reported on 20 June 2005 on an inspection of the use of Art. 96 alerts in the Schengen Information System. This report was presented to the Council of the European Union, The European Commission, the European Parliament and the national data protection supervisors. In that report, the JSA Schengen formulated seven recommendations to improve the implementation of and compliance with Art. 96 of the Schengen Convention.

In view of the importance of ensuring compliance - the vast majority (almost 90%) of Schengen alerts are Art. 96 alerts - the JSA Schengen decided in the spring of 2008 to check what has been done on a national level with the findings of the report, and which improvements have been achieved.

On 15 April 2008, the Chairman of the JSA Schengen sent a letter (ref. 08/04) to all members of the JSA Schengen who took part in 2004-2005 in the inspection on the use of Art. 96 alerts, requesting that the JSA Schengen be informed on the follow-up actions taken in their respective countries. The letter stressed the impact of being alerted for refusing entry, which might have serious consequences for an individual, especially in view of the problems detected in the inspections.

Recommendations

The 2005 inspection report recommended that:

- 1 Policy-makers should consider harmonising the reasons for creating an alert in the different Schengen States.
- 2 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.
- 3 The appropriate national authorities responsible for Art. 96 alerts should inspect these alerts on a regular basis.
- 4 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.
- 5 Authorities responsible for Art. 96 alerts should develop formal and written procedures to ensure that Art. 96 data are accurate, up to date and lawful.
- 6 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.
- 7 Measures should be implemented or further developed to prevent Art. 96 alerts on nationals from EU Member States.

Apart from the first recommendation, all recommendations can lead to national activities improving compliance with Art. 96 of the Schengen Convention. The first recommendation is directed towards the Schengen States and the European institutions.

Reactions received

Following its call to check the follow-up of its report, the Schengen JSA received 20 responses from the data protection authorities (DPAs) of: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Portugal, the Slovak Republic, Spain, Sweden, and Switzerland. Thirteen of those states participated in the Art. 96 inspection in 2004-2005. The other states used this opportunity to inspect the implementation of Art. 96.

This report does not present the experiences of two Schengen States¹ that participated in the 2004-2005 inspection.

The responses show a variety of activities undertaken to check the follow-up of the recommendations. In some states a written request was sent to the competent authority asking to be informed on activities implementing the recommendations; in others, a new inspection was organised to check whether improvements could be detected. The choice between these two approaches can be related to national practices when checking the follow-up of an earlier inspection, and the available capacity in the offices of the national supervisors. Other states chose not to do a specific follow-up action, as the findings in their first inspection did not show any specific data protection risks.

No specific follow-up actions took place after the Art. 96 inspection in eight Schengen states (Belgium, Finland, Iceland, Luxembourg, the Netherlands, Norway, Portugal, and Sweden). There were different reasons for this, for example:

- In Norway no follow-up check was deemed necessary as the competent authority for Art. 96 alerts – the Directorate of Immigration – fulfilled all necessary conditions at the time of the inspection (2005). In Belgium, Luxembourg and Sweden no specific problems were revealed during the inspection at national level, therefore no specific action was undertaken. The same is applicable for Iceland, as during its Art. 96 inspection in 2004–2005 the Icelandic DPA found out that the alerts on Art. 96 were used in conformity with the relevant rules. It should be mentioned that the Norwegian DPA considers that in view of the recent changes in the Norwegian legislation relating to the grounds for issuing Art. 96 alerts it would be interesting to perform a limited follow-up check on this topic.
- The Portuguese DPA advised that as the results of the Art. 96 national inspection were quite satisfactory, and no problems were encountered which were found in other Member States and which form the basis for the recommendations, there was no need for follow-up activities concerning Art. 96 alerts. During the national inspection the Portuguese DPA made one specific remark in the sequence of inspection, and this was immediately corrected.
- The Dutch DPA wrote to the responsible Minister in May 2008, referring to the conclusions and recommendations of the JSA Schengen following the inspection on the use of Art. 96. The answer from the Minister and state secretary of Justice related to both Art. 96 and Art. 99 investigations and recommendations, and advised that no changes would be made to the current situation, as it was not deemed appropriate to change the working methods regarding the current SIS, while awaiting the implementation of SIS II. It was noted that the recommendations of the JSA would be taken into account in the implementation of SIS II.

¹ No reactions received from France and Greece

Results

Results from DPAs that carried out specific follow-up actions², which relate to the recommendations, are presented here in the sequence of the recommendations.

1. Policy-makers should consider harmonising the reasons for creating an alert in the different Schengen States.

- In Germany, all cases examined in 2004, which lacked a sufficient reason for an alert, have been cleared. In order to avoid similar mistakes in the future, ministerial orders have been issued in two federal states. In three federal states the examination revealed that alerts were again issued without sufficient justification (e.g. foreigners who went underground and could not be expelled or deported).
- The Austrian SIRENE bureau is of the view that the reasons for alerting, based on Art. 96, are sufficiently harmonised by the Schengen Agreement and the SIS manual.
- The Italian DPA asked the Ministry for Home Affairs to issue written instructions to ensure that: decisions to enter SIS alerts are taken in all police offices by the head of the office and/or an officer specifically in charge of these; and that all alerts should be grounded in a decision containing specific reasons fulfilling the conditions laid down in the Schengen Convention. The DPA also requested that specific staff training sessions be organised, including at peripheral level. This information is also relevant to recommendation 5 (see below).

2. The 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.

- According to the Swiss answer, the comparison or approximation of the retention periods for SIS alerts in the national section of the SIS is performed continually and automatically.
- In Italy, data are retained for three years on the system; the offices that entered the alerts have to decide whether they should be renewed. This is an automatic procedure, in that each office receives a request to check the need for renewal one month prior to expiry of the given record. As for deportation measures, it should be clarified that the deadline set in Italian law is ten years from the time proof is provided that the alien left the Schengen territory; accordingly, the relevant SIS alert cannot be renewed pending the ban on the alien's entry.
- In the Czech Republic Art. 96 alerts not extended after the initial 3-year period are deleted automatically.
- In Germany, in most federal states, continued retention of data is reviewed after three years. In one federal state the obligation to review continued retention has been laid down in a decree. Three federal states report that due to insufficient documentation of reviews in the individual records it cannot be verified whether a review has taken place. Two data protection commissioners report that in the cases they examined no review was carried out after three years. In most cases in which the need for continued retention was reviewed after a period of three years such review was documented. However, reasons for extended retention are documented only in very few cases. On the question *what is the percentage of examined alerts where a) the alert may remain in effect for more than six years; b) the alert*

² Including results of inspections of Schengen States that were not involved in the 2004-2005 inspection.

may remain in effect for more than nine years; only three federal states answered this question. They all reported a number of alerts with retention periods of more than six years. In Germany, according to the answers received from three data protection commissioners the time limit for an alert in the SIS is linked to a permanent national ban on entry. Also, according to the answer received from Germany in those federal states for which information was provided records are not deleted after deletion of an alert from the SIS. Instead, documents remain in the foreigner's record and are kept for the purpose of documenting administrative action, among others.

Current practise of the issuing the alerts of Art. 96 which is being exercised by the Federal Police in Germany, SIS alerts for the purpose of refusing entry to third-country nationals are subject to the provisions of Art. 96 of the Schengen Convention.

The alerts issued by the Federal Police are based on the criteria for issuing alerts developed by the former Federal Police Central Bureau in Koblenz (Bundespolizeidirektion Koblenz) together with the Federal Ministry of the Interior in 1995 to provide a more precise definition of the term 'threat'; these criteria are still valid today. According to these criteria, an alert – especially an SIS alert – for the purpose of refusing entry may be issued with regard to third-country nationals if:

- they have stayed unlawfully in Germany for more than six months without the necessary residence authorisation;
- they are suspected of having committed document fraud, falsification of official identification cards, misuse of identification documents, procurement of fraudulent official identification cards (if such offences are relevant to their entry to and/or stay in the country), or procurement of visas under false pretences on several occasions, or to have been involved in the organised planning or implementing of illegal entry;
- there is a well-founded suspicion that they have initiated or facilitated the illegal entry and/or illegal residence of other foreigners;
- there is sufficient information indicating that they are pursuing terrorist aims or support terrorist activities;
- they have been convicted of a criminal offence that carries a sentence of at least one year's imprisonment;
- they are suspected of having committed serious criminal offences. For the purpose of alerts, criminal offences are deemed to be serious crimes if these offences were committed on repeated occasions in an organised manner and with considerable criminal energy.

In addition, the Federal Police issues alerts relating to third-country nationals under Art. 96(3) of the Schengen Convention in accordance with the conditions set out therein:

- Time limits
Initial alerts are generally limited to three years; they may be renewed only if the reasons that had led to the initial alert still remain.
- Documentation
A search record kept additionally to the information stored in the SIS contains complete documentation of all orders and instructions issued in relation to an alert.
- Post-deletion procedure
After an alert has been deleted, the corresponding record is retained for a certain period of time for documentation purposes. The length of time a record may be kept is subject to the retention periods set out in the order opening a CID Records Index.

- Austria advised that while alerts based on Art. 96 are stored in the SIS for a period of 3 years, national alerts do not expire until after a period of 6 years and 3 months. Therefore the retention periods in Austria are longer than those foreseen in the Schengen Convention, precluding the problematic situation that an alert nationally expired while still being valid for the SIS. Taking this into account a further harmonisation does not seem to be necessary (especially with regard to the foreseen automatic information of a scheduled deletion and the possibility for the extension of an alert in Art. 112 para 3 and 4 of the Schengen Convention).
- Spain advised that, according to the information provided, continued retention of data is reviewed after three years. A list of records reaching the limit is sent from the N-SIS management team to the competent authorities on a monthly basis in order to check if the alert should remain in effect. In this sense, it should be taken into account that, according to Spanish law, entry ban orders can be issued for a maximum of ten years.

3. *The appropriate national authorities responsible for Art. 96 alerts should inspect these alerts on a regular basis.*

- The Icelandic DPA reported that it calls each year for a report from the National Commissioner of the Icelandic police on an internal audit of the SIS in Iceland according to the national regulations. Switzerland indicated that SIRENE bureau inspects the alerts – including the alerts from the FOM (Federal Office of Migration) (majority of the issued alerts) – once a week.
- The Spanish DPA advised that it has been stated that those controls, even taking place regularly, are not subject to a formal interval on their execution; however, procedures affecting those regular inspections will shortly be released by COMI (the SIS coordination committee). Controls on Art. 96 alerts are conducted in the same way by the DPA inspection services in response to complaints investigation or requests for collaboration.
- The Austrian DPA advised that according to the "Fahndungs and Informationsvorschrift" (FIV 2009) the Austrian Foreigner's Offices (Fremdenbehörden) are obliged to inspect Art. 96 alerts on a regular basis (by all means every 3 years) with respect to lawfulness, 'up-to-date-ness' and accuracy. If necessary the correction or deletion of an alert has to be arranged.
- The Italian DPA advised that it asked its Ministry for Home Affairs to implement functions and tools to allow the monitoring of SIS accesses and the reporting of flaws and shortcomings. The necessary steps are being taken by the Ministry for Home Affairs. Once these new functions and tools are deployed, the DPA will be in a position to perform the required checks on a regular basis - also taking account of the audit logs. This information is also relevant to recommendation 6 (see below).

4. *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.*

- Austria advised that the subsequent joint inspections on several types of alerts conducted by the JSA Schengen together with the national DPAs have already applied questionnaires developed by the JSA Schengen, thus not only allowing the comparison of the different national results of the inspection but the comparison of inspections among each other.
- This subject will be dealt with by the JSA in the near future.

5. *Authorities responsible for Art. 96 alerts should develop formal and written procedures to ensure that Art. 96 data are accurate, up to date and lawful.*

- The Danish DPA informed that during the inspection carried out in the years 2004 and 2005 all the Danish Art. 96 alerts were reviewed by the National Commissioner of Police. After the inspection, the National Commissioner of Police indicated that the necessary steps had been taken to correct the errors identified during the inspection and that the internal guidelines concerning case handling and control procedures for the processing of cases that have to be reported under Art. 96 of the Schengen Convention would be further specified. The National Commissioner of Police asked the Director of Public Prosecutions to ensure that the prosecution services request correct orders for expulsions. The prosecutions services should also, when receiving the sentences passed, review them carefully, including their references to the expulsion provisions of the Aliens Act, in order to make sure that the expulsion orders that are part of the sentencing are correct viewed against the sentenced offences and, if required, the prosecution service must take steps to have such orders corrected. To accommodate the request of the National Commissioner of Police, the Director of Public Prosecutions by letter of 11th August 2005 informed the regional public prosecutors, the chief constables and the Commissioner of the Copenhagen Police of the problems and requested that the necessary checks, etc. were undertaken.
- According to the information provided by the Belgian DPA, in Belgium, an Art. 96 alert is only introduced in the SIS when a decision forbidding the entry on the Belgian territory for 10 years has been taken by the King or the Ministry for Home Affairs. In practice, this decision is taken when the data subject has been convicted for an offence carrying a penalty involving deprivation of liberty of at least one year. The national retention periods for national alerts cannot exceed 10 years. The Immigration service is the only service responsible for the processing of data related to Art. 96 alert.
- The Swiss DPA advised that the procedures for the Art. 96 alerts ordered by Federal Police (on demand of the Swiss Federal Directorate for Analysis and Prevention) are described in a SIS practical guide. The FOM (Federal Office of Migration) is responsible for its own alerts (majority of the alerts). Before transferring Swiss entry bans into the SIS, a user manual was established by the FOM which outlines all relevant steps, addressing also data quality issues.
- According to the information received from the Latvian DPA, the SIRENE bureau has to check data quality of an alert; if data are not correct, the SIRENE bureau of Latvia must inform the Office of Citizenship and Migration Affairs for correction.
- The Austrian DPA advised that formal written procedures to ensure that Art. 96 data are accurate, up-to-date and lawful are foreseen in the "Fahndungs und Informationsvorschrift" (FIV 2009). This instruction regulates the measures in connection with alerting searches and information in central information collections and obliges every Austrian Security Authorities and Foreigners' Offices. Additional rulings for authorities thus seem not to be necessary.
- The Spanish DPA advised that controls have been developed to check data before and after the insertion of the record in SIS. A common procedure for Art. 96 alerts has been included as part of the operative and best practices manuals issued by COMI (the SIS coordination committee). Additionally, database-level checks are carried out on a routine basis by the N-SIS management team. An issue to be taken into account comes from identity theft cases. Some requests for collaboration from other DPAs deal with this problem: an entry ban alert is included based on identity presumably obtained by means of an identity theft; when the person affected tries to obtain a visa, the request is denied because of a SIS alert associated with the requester. Although all known cases have been solved, some difficulties persist as a result of the forced delay due to the complexity of the process, which usually involves the

person affected, the DPA, the competent authority issuing the ban and the consular services of the Foreign Affairs Ministry.

- The Italian DPA adopted a decision in 2008 which includes instructions on the conditions to be fulfilled in order to extend, where necessary, the validity of SIS alerts, along with the determination of the data retention periods applying to the SIRENE division and the mechanisms for destroying any data that may not be kept for longer. A data quality procedure is implemented that relies on the measures recommended by the Strasbourg C.SIS. This automated procedure is published in the SIS area of the Schengen Portal created by the Ministry for Home Affairs. The portal also includes documents, guidance, online help tools and the relevant legislation. This information is also relevant to recommendation 6 (see below).

6. *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.*

- The Swiss DPA indicated that the SIRENE bureau would guarantee the quality and integrity of data, as well as for the double alerts of the FOM (Federal Office of Migration).
- The Austrian DPA advised that according to the FIV 2009 the authority responsible for the alert is obliged to inspect the lawfulness and the accuracy prior to storage in the central information collection. If a judicial authority is requesting a search, the authority responsible for the alert has to contact that judicial authority in case it doubts the accuracy of data in the request and this doubt is not based on evident mistakes in writing or in transmission. After the alert has been issued the responsible authority is obliged to check its accuracy via a query in the central information collection. Thus, without prejudice to alerting without delay if the minimum requirements have been met, the authorities responsible for the alert are obliged to correct or delete the data after an appropriate investigation has been conducted.

7. *Measures should be implemented or further developed to prevent Art. 96 alerts on nationals from EU Member States.*

- In the year 2007 – on the request of the Danish DPA – the Danish National Commissioner of Police checked if there were any Danish Art. 96 alerts concerning EU citizens. The result was negative; however, the check revealed some Art. 96 alerts concerning citizens from Switzerland. These alerts have now been deleted and the Danish National Commissioner of Police has informed the Danish DPA that no Swiss citizens will be subject to Art. 96 alert in the future.
- The Danish DPA carried out on 5 April 2005 an inspection on the use of information from the SIS by the Danish Immigrant Service.
- The Italian DPA carries out regular checks to ensure that no Art. 96 alerts are entered concerning EU citizens (except for aliases).
- In June 2007, the Belgian DPA checked Art. 96 alerts for EU citizens and did not find any except for aliases (3 Czechs, 1 Finn, 1 Hungarian, 3 Dutch).
- The Icelandic DPA also carried out checks on Art. 96 alerts on the nationals from the EU Member States. All Art. 96 alerts were reviewed by the Icelandic DPA and none of them were for EU citizens. Art. 96 alerts on Bulgarian and Romanian citizens were erased on the date these countries entered the EU.
- The Latvian DPA advised that no Art. 96 alerts have been placed on EU citizens.
- In February 2009, the Luxembourg DPA checked whether there were any Art. 96 alerts concerning citizens of the Schengen States. The result was negative. According to the

information received, regular controls as mentioned in the Schengen data protection evaluation report (dated 7 May 2009) will be carried on in the future.

- In Sweden the DPA regularly supervises the processing of personal data in the national SIS, approximately once a year, either by desk inspections or by on-site inspections. A simplified check of whether there were any Art. 96 data about EU citizens was done in 2007 by Swedish DPA. No such data were reported. In addition to that, a formal on-site inspection was carried out in May 2008. This inspection involved, among other things, a check of whether any Art. 96 data about EU citizens existed. The inspection confirmed the previous information that no Swedish entries according to Art. 96 referred to EU citizens. The National Police Board also gave a report on the procedures regarding the entry and further processing of Art. 96 data, including the measures that were taken to prevent such alerts about EU citizens.
- The Lithuanian DPA, while inspecting the Ministry of Internal Affairs and C.SIS under Art. 96 in 2009, also checked data on aliens for whom an alert has been issued for the purpose of refusing entry and found no data on EU citizens.
- According to the information provided by the Swiss DPA, there were no nationals from EU and other Schengen states in the SIS with a Swiss entry ban. Prior to the transfer of 'old' entry ban cases into the SIS, a list of those cases was established on the basis of a programme which generated all entry bans per country of origin minus EU and other Schengen countries. Any entry ban entered into the SIS by the Federal Office of Migration (FOM) following the operational access of Switzerland to Schengen in December 2008 excluded any EU or other Schengen nationality by default. The Swiss SISone4all mask is designed in such a way that it does not permit to enter EU and other Schengen nationalities.
- The Austrian DPA advised that by 1 September 2007 every single alert based on Art. 96 on nationals from Cyprus, Estonia, Latvia, Lithuania, Malta, Poland, the Slovak Republic, Slovenia, the Czech Republic and Hungary have been irreversibly removed from SIS. There is no indication (also during the national investigation of the DPA in February) for an alert on nationals from EU Member States recommending any necessity for further action concerning this issue.
- In Germany, no discrepancies were found. Whenever this question was raised in the follow-up check, it was noted that all persons concerned were either third-country nationals or nationals of the new accession states whose alerts would be deleted soon anyway.
- The Spanish DPA advised that controls have been established: prior to the insertion of the record, checks are performed in case of doubt (mainly possible dual nationality or issues related to used alias) and, as an additional control, routine checks searching for possible mistakes are carried out at database level. For example, the last check showed no Spanish Art. 96 alerts concerning EU citizens and just one record affecting a Spanish national, which had been included by the competent authorities of another country. The authority responsible for the record reported the existence of some doubts about the alleged nationality; this issue is still pending.
- In the Slovak Republic the system itself evaluates/checks if persons subject to Art. 96 alerts have citizenship of an EU Member State; if this is the case, such alerts are not sent into the SIS, even if all other conditions for creating the alert are met.
- In the Czech Republic, there are more stringent conditions on issuing alerts on those who are family members of EU citizens.

Schengen Data Protection Catalogue

In 2009, the JSA Schengen was involved in setting up a Schengen Catalogue³, recommendations and best practices on data protection. The catalogue was adopted by the Council of the European Union in 2010.

Most of the recommendations of the JSA Schengen are introduced in that catalogue as recommendations to be used when evaluating the implementation of data protection provisions of the Schengen Convention. It gives the Schengen States the opportunity to check compliance of the national activities and procedures with the data protection conditions related to Art. 96.

Raising awareness: other activities of national DPAs focused on raising awareness.

In Denmark, the Art. 96 inspection report was distributed to the National Commissioner of Police, the Ministry of Justice and the Danish Parliament (Folketinget). The results of the inspection provided to the National Commissioner of Police, concerning the results of Art. 96 inspection, were placed on the DPA's website. The Ministry of Justice was also informed of the results of the inspection.

The Icelandic DPA produced a brochure, which is available at the point at which air passengers enter the Schengen area in Keflavik international Airport.

The Swedish DPA reviewed and updated the information on its website regarding SIS earlier this year. There is a section with general information about SIS as well as a section with questions and answers regarding SIS. There are also links to other relevant information about SIS, including how to contact the National Police Board to demand access to information.

The Spanish DPA distributes relevant information concerning the issue to affected stakeholders through the N-SIS contact point. There are also regular contacts with the designated contact persons of the different police bodies; in the Schengen area of the Ministry of Interior; and the Ministry of Foreign Affairs. Relevant information has been published on the Spanish DPA's website, as well as the websites of the Ministry of Interior (www.mir.es) and national police (www.policia.es).

Conclusion

- This follow-up inspection, designed to check whether recommendations made following the initial inspection, has proven to be successful.
- While some Schengen states showed improved compliance, others have not implemented recommendations made. Gaps in compliance have been identified.
- Effective supervision and continuous attention to this issue is required from national data protection authorities and, importantly, from the relevant national authorities.
- This report will be distributed to relevant stakeholders in the Council, Commission and Parliament. It will also be sent to the relevant national authorities, in order to raise awareness and highlight the areas requiring close attention in their country.

³ Council doc. 9768/10.

ANNEX

Art. 96

1. Data on aliens for whom an alert has been issued for the purpose of refusing entry shall be entered on the basis of a national alert resulting from decisions taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.

2. Decisions may be based on a threat to public policy or security or to national security which the presence of an alien in national territory may pose.

This situation may arise in particular in the case of:

- a) an alien who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;
- b) an alien in respect of whom there are serious grounds for believing that he has committed serious criminal offences, including those referred to in Art. 71, or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a Contracting Party.

3. Decisions may also be based on the fact that the alien has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of aliens.

Art. 105

The Contracting Party issuing the alert shall be responsible for ensuring that the data entered into the Schengen Information System is accurate, up-to-date and lawful.

Art. 112

1. Personal data entered into the Schengen Information System for the purposes of tracing persons shall be kept only for the time required to meet the purposes for which they were supplied. The Contracting Party which issued the alert must review the need for continued storage of such data not later than three years after they were entered. The period shall be one year in the case of the alerts referred to in Art. 99.

2. Each Contracting Party shall, where appropriate, set shorter review periods in accordance with its national law.

3. The technical support function of the Schengen Information System shall automatically inform the Contracting Parties of scheduled deletion of data from the system one month in advance.

4. The Contracting Party issuing the alert may, within the review period, decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the technical support function. The provisions of paragraph 1 shall apply to the extended alert.

Art. 126

1. -

2. -

3. In addition, the following provisions shall apply to the automatic processing of personal data communicated pursuant to this Convention:

(a)

(b)

(c) the Contracting Party communicating such data shall be obliged to ensure the accuracy thereof; should it establish, either on its own initiative or further to a request by the data subject, that data have been provided that are inaccurate or should not have been communicated, the recipient Contracting Party or Parties must be immediately informed thereof; the latter Party or Parties shall be obliged to correct or destroy the data, or to indicate that the data are inaccurate or were unlawfully communicated;

d) -

(e) the transmission and receipt of personal data must be recorded both in the source data file and in the data file in which they are entered;

f)

4. This Art. shall not apply to the communication of data provided for under Chapter 7 of Title II and Title IV. Paragraph 3 shall not apply to the communication of data provided for under Chapters 2 to 5 of Title III.
