DATATILSYNET

Rigspolitichefen Afd. E, Udlændingeafdelingen (17 14 36 11)
Anker Heegaardsgade 5, 3
1780 København V

10. juni 2005

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2003-851-0048
Sagsbehandler
Jakob Gøtze Pedersen
Direkte 3319 3227

Undersøgelse af indberetninger i henhold til Schengen-konventionens artikel 96 - Rigspolitiets j.nr. 2004-5162-45

Den Fælles Tilsynsmyndighed Schengen har iværksat en undersøgelse af indberetninger til Schengen-informationssystemet (SIS) efter Schengen-konventionens art. 96 af uønskede udlændinge. I den forbindelse har Den Fælles Tilsynsmyndighed anmodet Datatilsynet om at undersøge, hvorvidt danske indberetninger vedrørende uønskede udlændinge, jf. Schengen-konventionens artikel 96, er sket i overensstemmelse med konventionen.

Baggrunden for Den Fælles Tilsynsmyndigheds initiativ er bl.a., at der kan konstateres store forskelle på antallet af indberetninger medlemslandene imellem. Eksempelvis havde Italien pr. 1. februar 2003 foretaget 335.306 indberetninger i SIS, Tyskland 267.884 indberetninger, Holland 9.363 indberetninger og Sverige 4.454 indberetninger.

I den anledning anmodede Datatilsynet ved brev af 21. september 2004 Rigspolitiet om at fremsende dokumentation for de indberetninger, der var sket fra dansk side i henhold til artikel 96 i 1. kvartal i 2004.

Ved brev af 28. oktober 2004 fremsendte Rigspolitiet det ønskede materiale.

Det fremgik heraf, at der i 1. kvartal 2004 i en række tilfælde fejlagtigt var sket indberetning til SIS.

På denne baggrund anmodede Datatilsynet ved brev af 17. december 2004 Rigspolitichefen om at gennemgå samtlige de indberetninger, der er sket fra dansk side i henhold til artikel 96, for at sikre, at der ikke i andre tilfælde fejlagtigt er sket registrering i SIS. Datatilsynet anmodede endvidere Rigspolitichefen om at oplyse, om de konstaterede fejl vedrørende indberetninger foretaget i 1. kvartal 2004 havde givet anledning til ændrede sagsgange, kontrolprocedurer eller lignende.

Ved brev af 3. maj 2005 er Rigspolitiet fremkommet med en udtalelse. Det fremgår heraf, at Rigspolitiet har gennemgået samtlige 443 sager, hvor udlændinge er blevet opdateret i SIS som uønskede, jf. udlændingelovens § 58 g.

Gennemgangen har omfattet de domme/administrative afgørelser, der ligger til grund for indberetningerne, registreringerne i Det Centrale Kriminalregister og SIS samt forkyndelsen for udlændingene af indberetningen til SIS.

Rigspolitiet har i forbindelse med gennemgangen af sagerne konstateret følgende:

- I 22 tilfælde er der fejlagtigt sket indberetning til SIS. Sagerne vedrører primært EU-statsborgere eller udlændinge, der er dømt for strafbare forhold, der ikke opfylder betingelserne i udlændingelovens § 58 g for indberetning i forhold til den pådømte lovovertrædelse eller straffens længde.

- I 17 tilfælde er der korrekt sket indberetning til SIS, men i forbindelse med opdateringen i SIS og Det Centrale Kriminalregister er der sket tastefejl, eller indberetningerne har ikke været fuldstændige i forhold til de obligatoriske felter, der skal udfyldes i SIS.

- I 7 tilfælde er der korrekt sket indberetning til SIS, men det har efterfølgende vist sig, at de pågældende var kendte under falsk navn, og dette er ikke blevet berigtiget i SIS, da man blev bekendt hermed, eller de pågældende er blevet indberettet under 2 identiteter.

- I 11 tilfælde er der korrekt sket indberetning til SIS, men der er fejlagtigt ikke taget skridt til, at Udlændingestyrelsen kan foretage konsultation i medfør af Schengen-konventionens artikel 25.

- Gennemgangen af de domme, der ligger til grund for indberetningerne til SIS, har endvidere vist, at dommene i 11 tilfælde er forkerte i forhold til udvisningsspørgsmålet. I 3 af de pågældende tilfælde er der – i overensstemmelse med indholdet af de afsagte domme – sket indberetning til SIS, men dommene har vist sig at være afsagt forkert i forhold til udvisningsspørgsmålet, og indberetningerne til SIS har som følge heraf ikke været korrekte. I 8 af de pågældende tilfælde har indberetning til SIS fundet sted i overensstemmelse med domfældelsen i forhold til det strafbare forhold i de afsagte domme, men henvisningerne til udlændingelovens udvisningsbestemmelser i dommene har været fejlagtige, således at dommene burde have været foranlediget berigtiget, førend indberetning til SIS fandt sted.

- I et mindre antal sager, hvor der er sket korrekt indberetning til SIS, har det vist sig, at forkyndelsen for udlændingen af indberetningen til SIS ikke har fundet sted i overensstemmelse med Rigspolitiets interne retningslinjer herom.

Rigspolitiet har oplyst, at man har taget de fornødne skridt til at rette de konstaterede fejl. Det er desuden oplyst, at de interne retningslinjer i Rigspolitiets Udlændingeafdeling vedrørende sagsgange og kontrolprocedurer i forbindelse med behandling af sager om indberetning i medfør af Schengen-konvention-ens artikel 96 vil blive præciseret.

Endvidere har Rigspolitiet anmodet Rigsadvokaten om at indskærpe over for politikredsene, at anklagemyndigheden i sager, hvor udvisning kan komme på tale, dels nedlægger en korrekt udvisningspåstand, dels ved modtagelse af afsagte domme nøje gennemgår disse, herunder henvisningen til udlændingelovens udvisningsbestemmelser, med henblik på at sikre, at dommenes afgørelse om udvisning er korrekt i forhold til det pådømte forhold, og om nødvendigt tage skridt til berigtigelse heraf.

I den anledning skal Datatilsynet – efter at sagen har været behandlet i Datarådet – udtale følgende:

1. I henhold til § 2, stk. 1, i lov om Danmarks tiltrædelse af Schengen-konventionen[1] gælder bestemmelserne i Schengen-konventionens afsnit IV (Schengen-informationssystemet) her i landet. Afsnit IV i konventionen omfatter artiklerne 92-119 og vedrører Schengen-informationssystemet.

Af § 2, stk. 2, i tiltrædelsesloven fremgår, at Rigspolitichefen er den centrale myndighed, der efter konventionens artikel 108, stk. 1, er ansvarlig for den nationale del af SIS.

Rigspolitiet er tillige dataansvarlig i forhold til persondatalovens regler og har i overensstemmelse med persondataloven anmeldt den nationale del af Schengen-informationssystemet til Datatilsynet.

Datatilsynet er tilsynsmyndighed i forhold til persondataloven og er desuden ifølge tiltrædelseslovens § 2, stk. 2, tilsynsmyndighed efter Schengen-konventionens artikel 114 og 128.

Datatilsynet påser ifølge persondatalovens § 58, stk. 1, af egen drift eller efter klage fra en registreret, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør af loven. Tilsynet kan efter lovens § 62 kræve enhver oplysning, der er af betydning for dets virksomhed.

Efter Schengen-konventionens artikel 114 fører Datatilsynet tilsyn med databasen i den nationale del af SIS og kontrollerer, at behandlingen og anvendelsen af de oplysninger, der er optaget i SIS, ikke krænker de berørte personers rettigheder. Til dette formål skal Datatilsynet have adgang til databasen i den nationale del af SIS.

Datatilsynet kontrollerede på baggrund af Den Fælles Tilsynsmyndigheds initiativ et udsnit af de danske indberetninger, nemlig de 20 indberetninger der var foretaget i 1. kvartal 2004.

Da dette udsnit viste, at der i en række tilfælde fejlagtigt var sket indberetning til SIS, anmodede Datatilsynet Rigspolitiet om at gennemgå samtlige de indberetninger, der er sket fra dansk side.

Rigspolitichefen har som ønsket af Datatilsynet gennemgået de nævnte sager. Datatilsynet har i den forbindelse noteret sig, at gennemgangen har omfattet såvel de domme/administrative afgørelser, der ligger til grund for indberetningerne, som registreringerne i Det Centrale Kriminalregister og SIS samt forkyndelserne for udlændingene af indberetningen til SIS.

Det er på denne baggrund Datatilsynets opfattelse, at Rigspolitiets redegørelse er egnet til at danne grundlag for tilsynets bedømmelse af de skete indberetninger.

2. Oplysninger om uønskede udlændinge, der nægtes indrejse, optages ifølge Schengen-konventions artikel 96 i SIS på grundlag af nationale indberetninger.

I Danmark findes kriterierne for indberetning af uønskede udlændinge i udlændingelovens § 58 g, og indberetningerne foretages af Rigspolitiet.

Ifølge udlændingelovens § 58 g indberetter Rigspolitichefen en udlænding, der ikke er statsborger i et Schengenland eller et land, der er tilsluttet Den Europæiske Union, som uønsket til Schengeninformationssystemet, hvis

1) udlændingen er udvist af landet i medfør af § 22, § 23 eller § 24, nr. 1,
2) udlændingen er udvist af landet i medfør af § 24, nr. 2, og den pågældende er idømt ubetinget straf af mindst 1 års fængsel eller anden strafferetlig retsfølge, der indebærer eller giver mulighed for frihedsberøvelse, for en lovovertrædelse, der ville have medført en straf af denne varighed,
3) udlændingen er udvist af landet i medfør af § 25,

[1] Lov nr. 418 af 10. juni 1997 om Danmarks tiltrædelse af Schengen-konventionen

4) udlændingen er meddelt afslag på opholdstilladelse efter § 10, stk. 1 eller 2, nr. 1 eller 2,
5) udlændingens opholdstilladelse er inddraget i medfør af § 19, stk. 2, nr. 2 eller 3, eller
6) udlændingen har fået udstedt visum efter § 4 eller § 4 a og er udvist af landet i medfør af § 25 b efter at have fået afslag på en ansøgning om opholdstilladelse efter § 7.

Det følger af udlændingelovens § 58 h, stk. 1, at Udlændingestyrelsen forestår konsultationer med myndighederne i et andet Schengen-land i medfør af Schengen-konventionens artikel 25.

Hvis Udlændingestyrelsen efter de i § 58 h, stk. 1, nævnte konsultationer finder, at en i medfør af § 58 g indberettet udlænding bør slettes som uønsket i Schengen-informationssystemet, sletter Rigspolitichefen ifølge § 58 h, stk. 2, den pågældende i Schengen-informationssystemet.

Det følger af Schengen-konventions artikel 105, at den indberettende kontraherende part har ansvaret for, at de oplysninger, der optages i Schengen-informationssystemet, er korrekte og aktuelle, samt at de er lovligt indberettet.

3. Datatilsynet må konstatere, at såvel den undersøgelse, der stikprøvemæssigt blev foretaget vedrørende 1. kvartal 2004, som den efterfølgende gennemgang af samtlige indberetninger, har vist, at der på en række punkter er sket fejl i de danske indberetninger til SIS.

Datatilsynet må således konstatere, at Rigspolitiet i et antal tilfælde har foretaget indberetning til SIS, uden at betingelserne i udlændingelovens § 58 g er opfyldt.

Herudover er det Datatilsynets opfattelse, at Rigspolitiet ikke har levet op til kravene i Schengenkonventionens art. 105, idet Rigspolitiet ikke har sikret, at de oplysninger, der optages i Schengeninformationssystemet, er korrekte og aktuelle, samt at de er lovligt indberettet.

Det er desuden Datatilsynets opfattelse, at Rigspolitiet ikke har levet op til persondatalovens § 5, stk. 4, hvorefter behandlingen af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysninger, og der endvidere skal foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Datatilsynet har noteret sig, at Rigspolitiet har taget skridt til at rette de konstaterede fejl.

Datatilsynet har endvidere noteret sig, at Rigspolitiet vil præcisere de interne retningslinjer vedrørende sagsgange og kontrolprocedure i forbindelse med behandling af sager om indberetning i medfør af Schengen-konventionens artikel 96.

Endelig har Datatilsynet noteret sig, at Rigspolitiet har anmodet Rigsadvokaten om at indskærpe over for politikredsene, at anklagemyndigheden i sager, hvor udvisning kan komme på tale, dels nedlægger en korrekt udvisningspåstand, dels ved modtagelse af afsagte domme nøje gennemgår disse, herunder henvisningen til udlændingelovens udvisningsbestemmelser, med henblik på at sikre, at dommenes afgørelse om udvisning er korrekt i forhold til det pådømte forhold og om nødvendigt tage skridt til berigtigelse heraf.

4. Sammenfattende kan Datatilsynet konstatere, at der i de 443 danske indberetninger af uønskede udlændinge til SIS er sket fejlagtig indberetning i 25 tilfælde, og at der herudover er sket forskellige fejl i yderligere et antal tilfælde.

Indberetningerne til SIS vil kunne få alvorlige konsekvenser for den pågældende person, idet en person efter konventionens artikel 5 som hovedregel ikke vil kunne få tilladelse til at indrejse i og opholde sig i Schengen-området.

På den baggrund er det Datatilsynets opfattelse, at der er tale om et uacceptabelt højt antal fejl, og tilsynet finder således resultatet af undersøgelsen kritisabelt.

5. På denne baggrund har Datatilsynet i brev af dags dato orienteret Justitsministeriet om de konstaterede tilsidesættelser af Schengen-konventionen, udlændingeloven og persondataloven.

6. Datatilsynet forventer at offentliggøre dette brev på sin hjemmeside. Tilsynet vil endvidere orientere Den Fælles Tilsynsmyndighed om resultatet af gennemgangen.

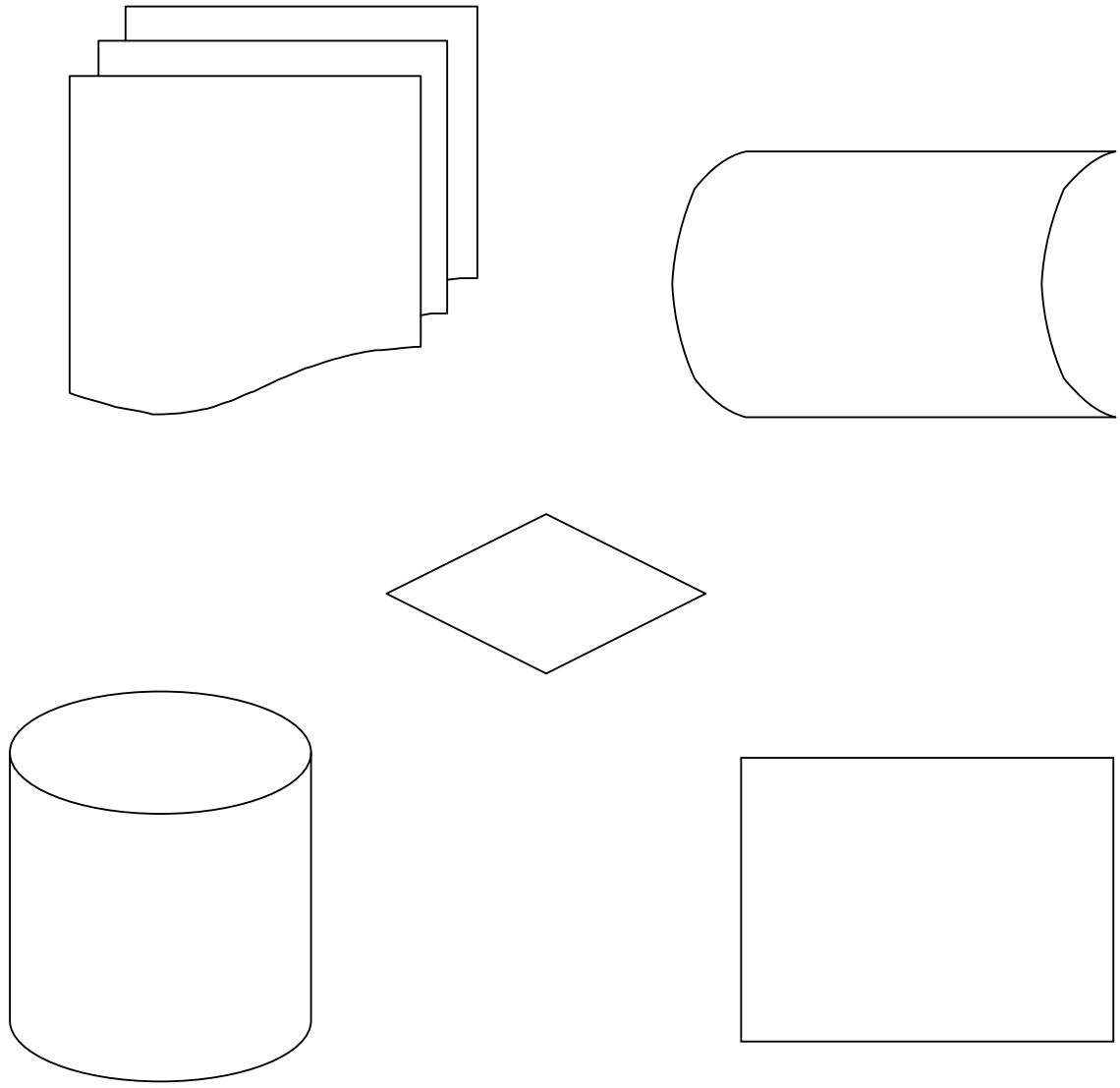
Med venlig hilsen

Asbjørn Jensen
Formand for Datarådet

Janni Christoffersen
Direktør

ARTICLE 96 INSPECTION

Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System



Brussels, 20 June 2005

I. Introduction

The Schengen Information System (SIS) processes data on more than one million persons,[2] and in almost 90% of cases these data concern Article 96 alerts – alerts on third-country nationals refused entry to the Schengen area.

At the request of the Schengen Joint Supervisory Authority (JSA), the national data protection authorities have inspected those Article 96 alerts entered in the SIS by the competent authorities in their respective countries. The findings of these inspections were provided to the JSA and, in this report, the JSA presents an evaluation of the results.

II. Data Protection Supervision

Following the provisions of the Schengen Acquis, [3] personal data are processed in the SIS by the 15 participating states (the Schengen States). The Schengen Acquis divides the data protection responsibilities for the content and the functioning of the SIS between national data protection authorities and the JSA. The Schengen State that entered the data in the system is responsible for the processing of those personal data in the SIS, and the national data protection authorities supervise this. The JSA has to supervise the technical support function of the SIS. This function is supposed to ensure that data entered in the SIS are distributed to all Schengen States.

Article 115 of the Schengen Convention describes the tasks of the JSA. Apart from checking the technical support function of the SIS, the JSA is charged with examining any difficulties of application or interpretation that may arise with the operation of the SIS, as well as drawing up harmonised proposals for joint solutions to existing problems.

III. Reason for inspection

At the JSA meeting on 7 March 2003, some concerns were raised about Article 96 alerts. Various publications suggested that Schengen States might be creating alerts on individuals other than those provided for under Article 96 – such as anti-globalisation demonstrators.

[2] Records on persons and alias data
[3] OJ.L 239, 22/09/200

There was also a need to establish whether the variations in the number of Article 96 alerts entered by the different Schengen States was the result of Article 96 being applied differently. Other factors that might explain the variations include differences in national law, differences in the way the competent national authorities operate in practice, differences in immigration flows or even the political situation in a particular state. Nonetheless, the possibility that Article 96 is being interpreted differently throughout the Schengen area should not be ruled out. In view of this, the JSA decided to request the national data protection supervisors to inspect the national SIS in a joint action.

IV. Scope and method of inspection

The objective of the inspection was to ensure that Article 96 data were being processed in accordance with Article 96, the data protection principles in the Schengen Convention, the SIRENE Manual and the applicable national legislation. The method of the inspection should also make it possible for the JSA to assess whether interpretation problems exist on the use of Article 96.

For that purpose the JSA, assisted by a group of experts of the national data protection authorities, developed a model for inspection to be used by all national data protection authorities. Using this model would enable the JSA to compare results.

The model was composed of a questionnaire and two inspection modules (see annexes).

The questionnaire aimed to get an overview of the relevant national law in the Schengen States, and it provided the national data protection authorities with the necessary information to start the inspection.

Module I was developed as an instrument for the national data protection authorities to check all procedures necessary to fulfil the data protection requirements by authorities responsible for alerting individuals according to Article 96.

Module II was developed as a guideline for the national data protection authorities to check the content of the Article 96 alerts. This module helped to establish whether the alerts were in accordance with the provisions of Article 96 and whether they were maintained in the SIS in accordance with the provisions in the Schengen Convention.

V. Reactions received

The data protection authorities in all Schengen States participated in this inspection. This coordinated effort underlines the importance that national data protection authorities place on inspecting the application of Article 96 alerts.

VI. Results and evaluation module I

The JSA has assessed the results of the inspections according to the two different modules. In the presentation of this assessment the JSA emphasizes some guiding principles for the use of Article 96 alerts. It should be stressed that although the national data protection authorities use the same model of inspection, there might be differences in approach and in the way the results are reported. In some cases an inspection had already taken place just before the model was developed. The results of these earlier inspections were then used when answering the questions in the model. In view of this, the JSA has limited the presentation and evaluation to those subjects where it was possible to make a comparison.

The evaluation concerns three aspects of the inspection:

A. Conditions of Article 96

B. Specifics

C. Explanation of the difference in numbers of alerts.

A. Conditions of Article 96

Before an Article 96 alert may be processed in the SIS there has to be:

1. A decision taken by a competent administrative authority or court.

While immigration law and immigration authorities obviously play a major part in the decision leading to an Article 96 alert, this area is governed by a variety of laws and is administered by a number of different authorities in the different Schengen States. Authorities listed include the courts, the police, ministries of interior and justice; and the different laws applicable include penal law, tax law, and laws on public order and national security.

In Greece, Spain, Sweden, Germany, Denmark, France and Portugal a court decision may also lead to expulsion.

2. That decision must result in a national alert to refuse entry.

In eleven Schengen States the decision leads automatically to a national alert. In some Schengen States a separate decision is necessary. In one Schengen State the condition for a national alert is not applied.

3. A decision must be made to enter these data in the SIS as an Article 96 alert.

Most answers received indicate that a decision is made to enter the data in the SIS. However, there is a difference in responsibility. In some Schengen States it is the authority responsible for the original decision, whereas in other Schengen States it is the authority responsible for the processing of data. In two Schengen States a decision to refuse entry will automatically lead to an Article 96 alert. Although a separate decision is required to enter an alert on a person in the SIS, the results of the inspection indicate that in practice in most cases a decision to refuse entry will almost automatically lead to a decision to create an Article 96 alert. A national alert should not become a SIS alert unless it satisfies all the conditions of Article 96.

4. Data should be accurate, up to date and lawful

According to Article 105 data must be accurate, up to date and lawful. The question asked in the inspection was whether there was a formal description of the procedure to process these data in the SIS and to ensure that data were accurate, up to date and lawful. In six cases reference was made to an NSIS users guide or SIRENE handbook. This refers to the SIRENE Manual as adopted by the Council. In two answers reference was made to the SIS and in one case no formal description was present. In four cases reference was made to internal procedures. In two cases the question was answered by a "yes" without stating the specifics of the formal description.

It is clear that where data are processed by different organisations, or by different departments of one organisation as parts of one chain of processing, it is essential to have specific procedures in place to keep data accurate, up to date and lawful. The SIRENE Manual, which sets out the rules and procedures governing bilateral or multilateral exchange of supplementary information,[4] cannot be seen as a procedure to ensure that data are accurate, up to date and lawful.

5. The storage of data should be reviewed periodically (Article 112)

In most answers reference was made to the warning system of the SIS. In one state the review procedure is not entirely formalised. In another state a check is made every two years.

[4] Article 1 of the SIRENE Manual

B. Specifics

1. Overview systems used for data processing and the responsible authorities.

The different stages of processing personal data (processing decision and time limit, processing as national alert and processing in SIS) may be regarded as different parts of a chain.

The way it is ensured that data are accurate and up to date depends on the way the chain is organised and how (different) responsibilities are interlinked. In seven Schengen States one authority is responsible for the whole chain. In the remaining Schengen States different authorities are responsible for the different stages of processing.

2. Time limit to refusal entry / processing of alerts

Most decisions have a time limit that exceeds the limit set by Article 112 of the Schengen Convention. However, in France, Sweden and Portugal time limits of less than three years are possible. The time limit in Iceland is related to the period referred to in Article 112 of the Schengen Convention. In most Schengen States the time limit is processed in the systems used to process data on the decision, the national alert and the SIS. In most Schengen States the retention period in the different systems is the same as the time limit for refusal entry. In one Schengen State, the national data protection authority has recommended to formalise the procedure for reviewing.

Since the time limits are related to the legal instrument used to refuse entry, and in view of the diversity of legal instruments and retention periods in the Schengen States, individuals might be refused entry for the same reason but for different periods depending on the Schengen State responsible for the decision.

C. Explanation of the differences in numbers of alerts

The results of the inspection indicate different factors creating the sometimes significant differences in numbers of alerts. While immigration law and authorities obviously play a major role in the process leading to an Article 96 alert, this area is also governed by a variety of other laws and is administered by a number of different authorities in the Schengen States. This, combined with the existence of different authorities responsible for the processing of personal data relating to an Article 96 alert, might go some way to explaining the significant differences in numbers of alerts (there are of course other factors, such as migratory flows). Furthermore, the lack of sufficient procedures to ensure that data are kept accurate and up to date might create a situation in which alerts are proc-

essed in cases where there have been no checks made to ensure that processing remains necessary for the purposes of Article 96.

The different retention periods in Schengen States also creates a situation in which an alert entered in similar cases by certain states will remain in the SIS for longer than had it been entered by another state with a shorter retention period. It should also be noted that in some Schengen States the decision to alert someone in the SIS follows automatically from a decision to refuse a person entry to that Schengen State. Such a system, where national alerts are entered in the SIS as a matter of course, is more likely to result in the creation of unwarranted alerts in the SIS.

VII. Results and evaluation module 2

This module focused on checking the content of Article 96 alerts.

Reports on the results of this inspection were received from Luxembourg, Iceland, Holland, Spain Belgium, Denmark, Italy, Sweden, Greece and France.

In this check, national data protection authorities checked the content of the alert and the file supporting the alert. It should again be stressed that the results only present an indication whether the checked Article 96 alerts fulfil all the conditions set out in Article 96 and the applicable national laws. In view of the differences in the number of alerts entered by each Schengen State, and the differences in capacity available to conduct the inspection, no scientific based statistics will be presented. For example, in one Schengen State checks using a sample of 2 % of their alerts led to a check of 240 dossiers, whereas in another case a 5% check involved only 20 dossiers.

Based on the results reported to the JSA three categories of problems may be identified in relation to the content of the Article 96 alerts.

i) Alerts not in conformity with the national law. In these cases the conditions set out in the national law were not complied with.

ii) Errors when entering the final date of the alert. This concerns errors on a national level (national databases) which can result in an incorrect period of retention, with data often being held for longer than necessary.

iii) Alerts on nationals from EU Member States.

In one case, the results on the inspection of the alerts caused a national data protection authority to request the authority responsible for Article 96 alerts to examine all entries made by that authority.

No reports were received that data were processed on so called anti-globalisation demonstrators.

VIII. Considerations and recommendations

One of the characteristic features of the SIS is the shared responsibility for using such a system in accordance with the provisions set out in the Schengen Acquis and national laws. The acquis is also the first common legal instrument with specific data protection provisions on the use of the SIS. The joint effort of the national data protection authorities to check the national Article 96 contributions to the SIS in a certain period and using the same model for inspection emphasizes a joint concern for the proper use of the SIS. This joint action perhaps marks a milestone in cooperation between national data protection authorities in the European Union. This first joint action underlines the need to invest in establishing a framework for data protection inspections in those areas where cooperation between EU Member States leads to the processing of personal data.

In view of the findings of the Article 96 inspection, the JSA makes the following recommendations:

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

Annexes

I. Article 96 Inspection

The model for inspection seeks to ensure that Article 96 data are processed in accordance with the privacy related legal norms and the data protection principles in the Schengen Convention, the SIRENE Manual and the national legislation.

The objectives and the scope of the inspection of Article 96 data are defined on basis of the Articles 96, 105, 112 and 126 of the Schengen Convention (OJ L 239, 22.09.2000, pag.19) and the SIRENE Manual (OJC, 38, 17.02.2003, pag 1)

Different authorities are involved with the processing of Article 96 data. The questionnaire used to inventory the different laws and authorities involved with Article 96 demonstrates a variety of applicable laws and authorities responsible for the processing of personal data. In view of this variety it is necessary to distinguish two specific scopes of the inspection. The first scope is to check if all the authorities involved with Article 96 data have taken sufficient actions to ensure that these data are processed in accordance with the applicable legal norms and data protection principles. The second scope is to check the content of the Article 96 data.

In view of this, the inspection is divided in two modules, each module suited to be used separately from the other. These modules aim at introducing a similar method of inspection anticipating the national practice of data protection inspections.

The great advantage of using the same model for inspecting the Article 96 data by all data protection authorities of the EU Member States participating in the Schengen Convention is to allow a comparison of the practice and use of these alerts in the different States. It allows the JSA Schengen and the national data protection authorities to have an overview on how Article 96 of the Schengen Convention is implemented in the different national frameworks.

This model has been developed in co-operation with the technical experts group established to assist the joint supervisory authorities.

II. Modules

Two modules are developed:

Module 1 is developed as an instrument for the national data protection authorities to check all procedures necessary to fulfil the data protection requirements by the authorities responsible for alerting individuals according to Article 96.Where different authorities are involved, this module may be used checking all these authorities individually. The structure of the module allows national data protection authorities to receive information on the implementation of data protection principles with the authorities or organizations involved with the Article 96 alerts. It does not interfere with the different practice of inspections in the Member States.

Module 2 is developed as a guideline for the national data protection authorities to check the content of the Article 96 alerts in order to establish if they were alerted in accordance with the provisions of Article 96 and if they are maintained in the SIS in accordance with the provisions in the Schengen Convention.

Module 2 builds on the results of module 1

In the future a module could be developed for a full privacy audit.

Module 1

Check all procedures necessary to fulfil the data protection requirements at the authorities responsible for alerting individuals according to Article 96. This module may be used as a questionnaire to be send to the authority responsible for the processing of data relating to the decision or used as a question list in interviews.

Before an Article 96 alert may be processed in the SIS, there has to be

1. A decision taken by a competent administrative authority or court.
2. That decision must result in a national alert to refuse entry.
3. A decision must be made to enter these data in the SIS as a Article 96 alert.
4. According to Article 105 it should be ensured that these data are accurate, up-to-date and lawful
5. The storage of data should be reviewed periodically (Article 112)
6. According to Article 126, (3c) the accuracy should be ensured and in case of inaccuracies, the recipients of these data should be informed.

1. A decision taken by a competent administrative authority or court.
(This list is focussed on the authority and the organization in which it operates dealing with the decisions resulting in national alerts for refusing entry)

1. Name of the authority:
2. Name of the organization in which the authority operates:
3. Name of the authority that according to the national data protection law is responsible for the processing of data:

A. Organization structure

1) a. Is there an up-to-date and formal description of the organization responsible for processing the alert data?: yes/no *
b. If yes please note the name or number of the source document:.....
c. If not, give a short description of the organization:.....

* (If different organisations are involved, this question applies to all)

Decision refusing entry	**Processing of personal data**
B. I. Content of the decision 1) a. Does the decision contain the reason for the decision?: yes/no b. Does the decision explicitly mention that entry to the Member State is refused?: yes/no c. If the decision explicitly refuses entry is there a time limit for this refusal?: yes/no d. If there is a time limit, what is it?:..... e. If there is a time limit, is it extendable?: yes/no d. If the time limit is extendable, for what period?:.....	**B. II. Processing of data concerning the decision** 1) a. In which system is the decision registered?:..... b. Who is responsible for the processing of these data?:..... c. Is the refusal of entry as such registered and if so in which system?:..... d. If there is a time limit, is that registered and if so in which system?:..... e. What is the retention period for the data mentioned: under a::..... under c::..... under d::.....

C. I. Decision to refuse entry	**C.II. Processing of personal data**
1). If the decision mentioned under B contains a decision that entry is to be refused and this automatically leads to a national alert refusing entry: (if not, continue with question C.2)	1). a If yes, where are these data processed?.....
a. Is the authority responsible for the processing of the alert-data the same as that responsible for the processing of data relating to the decision?: yes/no b. If the decision to refuse entry does not contain a time limit, is there a limit for the processing of these data?: yes/no	
c. If yes, what is this time limit?:..... d. If there is a time limit, is it extendable?: yes/no	b. Is this time limit explicitly registered?:.....
e. If the time limit is extendable, for what period?:.....	c. Is the extension of this time limit explicitly registered?:.....
2) If the decision mentioned under B contains a decision that entry is to be refused but an alert refusing entry needs a separate decision:	2)
a. Which authority decides on issuing an alert?..... b. Does this authority belong to the organization responsible for the processing of data relating to the decision?: yes/no	a. In which system is the decision registered?.....
c. If not, which authority is responsible?:..... d. On what legal grounds is such a decision taken?:..... e. Does the decision to refuse entry have a time limit?: yes/no	b. Is this time limit explicitly registered?:.....
f. If there is a time limit what is it?:..... g. If there is a time limit, is it extendable?: yes/no	c. Is the extension of this time limit explicitly registered?:.....
h. If the time limit is extendable, for what period?:....	
3) If the decision mentioned under B does not contain a decision that entry is to be refused:	3). a. In which system is the decision registered?.....
a. Which authority decides on issuing a national alert?:..... b. Does this authority belong to the organization responsible for the processing of data relating to the decision?: yes/no	
c. If not, which authority is responsible?:.....	

d. On what legal grounds is such a decision taken?:..... e. Does the decision to refuse entry have a time limit?: yes/no f. If there is a time limit what is it?:..... g. If there is a time limit, is it extendable: yes/no h. If the time limit is extendable, for what period:.....	b. Is this time limit explicitly registered?:..... c. Is the extension of this time limit explicitly registered?:.....
D.I. National alert 1) When a national alert is processed in the system mentioned under C.II., question 3 a, who is responsible for ensuring that these data are accurate, up-to-date and lawful?..... 2) Is the retention period for these data the same as mentioned under B II, question 1 e: a. the same period:..... b. a longer period:..... c. a shorter period:..... 3) If the retention period is longer, how is it ensured that these data are accurate, up-to-date and lawful?..... 4) If the time limit of the refusal entry is shorter then the retention period mentioned under 3, is the alert deleted after that time limit has expired?..... 5) If the answer to question 4 is negative, how is it ensured that these data	**D.II. Processing of personal data** 1) a. Is a reference to the formal decision to refuse entry processed in the system?..... b. If no reference is processed, is there another method of checking the data processed with the original decision?..... 2) a. Is there an automatic system for deletion of the data after the retention period has expired?..... b. If such a system exists does it automatically delete the data or is a warning for deletion foreseen?.....

are accurate, up-to-date and lawful.....	
E. I. Schengen Article 96 alert 1) Which authority decides to enter the alert in the Schengen Information System? ..... a. is this the same authority as mentioned under B.II,.nr 1,b.....yes/no C. I, nr.1.c.....yes/no C. I, nr.1.d.....yes/no C. I, nr.2.a.....yes/no C. I, nr.2.c.....yes/no C. I, nr.3.a.....yes/no C. I, nr.3.c.....yes/no Another authority..... 2) Is the authority mentioned under question 1 the same as the authority responsible for the processing of personal data by the national SIRENE bureau ?.yes/no a. If no, who is responsible for SIRENE?..... 3) Is there a formal description of the procedure to process these data in the Schengen Information System and to ensure that these data are accurate, up-to-date and lawful?? 4) On what grounds is such a decision taken?..... 5) What is the formal procedure for the review of data (Article 112(1))?..... 6) Is there a shorter review period then 3 years (Article 112 (2))?.....	**E. II. Processing of personal data**

7) Is the review period the same as mentioned under B II, question 1 e: a. the same period:..... b. a longer period:..... c. a shorter period:..... 8) If the period for processing the Article 96 alert is extended: a. Which authority is responsible for that decision?..... b. Which procedure is used to check the necessity of the extension of the period of processing the Article 96 alert?..... c. Does this procedure also involves a check with the decision refusing entry?.....	

F. Conclusions

Do the answers on the questions B.I-E.I in connection with the answers to B.II-E.II demonstrate a structured processing of Article 96 data with the guarantee that:

a. The data are accurate.
b. The data are up to date.
c. The data are lawfully processed.
d. The data are retained within the applicable (national) time limits.
e. The transmission of data is recorded.

Module II

The purpose of this module is to provide guidelines for checking the content of Article 96 data in the National Schengen Information System.
It is left to the national supervisors to select the data that will be subject of a check. This module builds on the results of the check as described in module I.
This module distinguishes the following steps:

A. Content of the alert

1. Is the content in conformity with Article 94 and Article 96.
2. No data may be processed of nationals of the Schengen States.

B. Content of the file

1. Is there a file at the SIRENE bureau (see module I, point E.I and SIRENE manual Article 3.1.6)
1.a Check the content of the file.
2. Is there a file at the authority mentioned in module I, point D.I)
2a. Check the content of the file.
3. Is there a file at the authority mentioned in module I, point C.I)
3a. Check the content of the file.

4. Is there a file at the authority mentioned in module I, point B.I)
4a. Check the content of the file.

C. Results
1. Does the check under A and B demonstrate that
a. The data are accurate.
b. The data are up to date.
c. The data are lawfully processed.
d. The data are retained within the applicable (national) time limits.
e. The transmission of data is recorded.
f. The alert is still necessary.

ANNEX

Article 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 Article 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.

Article 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.

Article 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 Article 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.

Article 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 Article 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.