COUNCIL OF
THE EUROPEAN UNION

Brussels, 10 May 2010

9768/10

SCH-EVAL 55
COMIX 361

**NOTE**

| | |
|---|---|
| from: | Drafting Group for Schengen Catalogue on Data Protection |
| to: | Schengen Evaluation Working Party |
| Prev. doc. nº: | 10841/2/09 REV 2 SCHEVAL 83 COMIX 485 |
| Subject: | Catalogue of recommendations for the correct application of the Schengen acquis and best practices: data protection |

# 2010

# SCHENGEN CATALOGUE

## RECOMMENDATIONS AND BEST PRACTICES

# DATA PROTECTION

**TABLE OF CONTENTS**



*

* *

## I. INTRODUCTION

1. At its meeting on 28 May 2001, the Council set as an objective for further work by the Working Party on Schengen Evaluation the identification of "... best practices, particularly as regards border controls, so that they can serve as examples for those States acceding to Schengen but also those fully applying the Schengen acquis. These evaluations and the identification of best practices shall serve as inspiration for the establishment of standards defining the minimum application of the Schengen acquis (…) in the relevant working groups" (mandate for the Working Party on Schengen Evaluation) (8881/01 – SCH-EVAL 17, COMIX 371).

   On the basis of this mandate, the Working Party on Schengen Evaluation worked out the principles and procedure for drawing up a catalogue of recommendations for the correct application of the Schengen acquis and of best practices, hereinafter referred to as the catalogue of recommendations and best practices, or catalogue.

   The purpose of the catalogue is to clarify and detail the Schengen acquis and to indicate recommendations and best practices, in order to provide an example for Member States and associated countries not (yet) applying the Schengen acquis in full and also those applying it fully. The aim is not to provide an exhaustive definition of the whole of the Schengen acquis but to put forward legally non-binding recommendations and best practices in the light of the experience gained by the Working Party on Schengen Evaluation in verifying the correct application of the Schengen acquis in several countries.

   The text of the catalogue does not seek to introduce new requirements but should make it possible to draw the Council's attention to the need, where appropriate, to amend certain provisions of the Schengen acquis so that the Commission and, where appropriate, the Member States take the recommendations and best practices into account when putting forward proposals or formal initiatives.

   Moreover, the catalogue should serve as a reference tool for evaluations. It may therefore also serve as an indicator for candidate countries of the tasks which they will be assigned.

2. The Working Party on Schengen Evaluation adopted the following definitions to conduct this exercise:
   recommendations: non-exhaustive series of measures which should make it possible to establish a basis for the correct application of the Schengen acquis and for monitoring it.
   best practices: non-exhaustive set of working methods or model measures which must be considered as the optimal application of the Schengen acquis, it being understood that several best practices are possible for each specific part of Schengen cooperation.

3. In 2002-2003, four volumes of catalogues were produced with regard to the application of the Schengen acquis: on external borders, removal and readmission (volume 1), on the Schengen Information System/Sirene (volume 2), on the issuing of visas (volume 3) and on police cooperation (volume 4).

4. At its meeting on 17 July 2008, the Working Party on Schengen Evaluation set the objective of revising and updating the existing catalogues to reflect the legislative, organizational and technical developments in the areas covered by the catalogues since the time of their first publication. At the same time, a decision was taken to produce a new catalogue covering data protection issues stemming from the Schengen acquis.

5. The task of producing the new catalogue on data protection was assigned to an expert group led by Belgium, which launched its activities under the French Presidency. The Czech Presidency continued work on the new catalogue and took over the leading role in drafting it.

6. After an in-depth discussion about the scope of the catalogue, relating in particular to the VIS and the new SIS, the Working Party on Schengen Evaluation agreed to proceed on a step-by-step basis and to produce a new catalogue in two phases: first gathering information from Schengen evaluation reports and providing for an overview of recommendations and best practices applying to currently valid rules (phase 1) and then complementing such a catalogue with recommendations concerning SIS II and VIS at a later stage, once available (phase 2).

7. Therefore the present catalogue constitutes a provisional version of the catalogue, to be finalised in due time. The catalogue reflects the extensive experience gained in Schengen evaluations of data protection in the recent past, in terms of recommendations and identified examples of best practices and in terms of the experiences of the Schengen Joint Supervisory Authority.

8. The primary focus of this catalogue is the protection of personal data within the Schengen Information System and the related general rules applying to personal data protection in terms of national legislation, national supervisory authorities, etc. In this respect, the Catalogue covers all relevant rules governing personal data protection vis-à-vis SIS as laid down by the Schengen acquis, including non-legislative and implementing measures which affect the use of the SIS by all authorised authorities: security measures, technical requirements for IT systems, confidentiality, rights of data subjects, public awareness etc.

9. The catalogue should be read in conjunction with other volumes of updated catalogues containing recommendations and best practices concerning data protection, in particular the catalogues on SIS and issuing of visas.

## II. RECOMMENDATIONS AND BEST PRACTICES

| **RECOMMENDATIONS**<br><br>***"a non-exhaustive series of measures which should make it possible to establish a basis for the correct application of the Schengen acquis and for monitoring it"*** | **BEST PRACTICES**<br><br>***"a non-exhaustive set of working methods or model measures which must be considered as the optimal application of the Schengen acquis, on the understanding that more than one best practice is possible for each specific part of Schengen cooperation"*** |
|---|---|
| **1. LEGISLATIVE BACKGROUND** | |
| ***1.1.*** **Legislation**<br>*Art. 117, 126 and 127 of the Convention from 19 June 1990 implementing the Schengen Agreement of 14 June 1985 (hereafter "CISA" or "the Schengen Convention")* | |
| - The national legislation providing for rules on personal data protection with regard to data processing in the SIS fully complies with the Council of Europe Convention for the Protection of Individuals with regard to Automatic processing of Personal Data of 28 January 1981 and the additional protocol to that Convention of 8 November 2001; furthermore it is 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;<br><br>- specific national legislation can supplement or clarify data processing in the SIS where necessary;<br><br>- supplementary and/or subsidiary legislation should not intervene or undermine the powers and competences of the national supervisory authority relating to the SIS;<br><br>- the Council Framework Decision 2008/977/JHA on the protection of | - The right to the protection of personal data is guaranteed by law as a fundamental right. |

| | |
|---|---|
| personal data processed in the framework of police and judicial cooperation in criminal matters must also be respected (from 27 November 2010; assessed as supporting document only, since it is not applicable to data processing in the SIS);<br><br>- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data has to be implemented as well (assessed as supporting document only, since it is not applicable to data processing in the SIS). | |
| ***1.2.*** **Bilateral and multilateral agreements (between Member States and third countries)** *(governed by international law)* | |
| - All bilateral or multilateral agreements with third countries concerning data processing in the area of police and judicial cooperation in criminal matters should contain provisions on data processing in compliance with obligations arising from the Schengen acquis;<br><br>- applicable standards of data protection (based on the Council of Europe Convention No. 108 and its additional Protocol of 2001 and the Council Framework Decision 2008/977/JHA) must be respected; | - Standard data protection clauses should be used in the agreements ensuring effective data protection[1]. |

[1] Resolution of the Spring Conference of the European Data Protection Commissioners (Edinburgh, 24 April) on bilateral and multilateral agreements between European states and third countries in the area of police and judicial cooperation in criminal matters.

| **2. NATIONAL SUPERVISORY AUTHORITY**<br>*Art. 114 sec. 1 CISA* | |
|---|---|
| *2.1.* **National Supervisory Authority – independence** | |
| - The national supervisory authority is an independent supervisory authority responsible for protecting the principles of personal data protection contained in the national legislation and in the Schengen Convention;<br><br>- the independence of the national supervisory authority must be ensured by legal, institutional and operational guarantees;<br><br>- institutional independence is ensured if the national supervisory authority is established in such a way that no hierarchy exists with public authorities responsible for processing the data in the SIS; a clear administrative statute should highlight this aspect of its independence;<br><br>- legal independence consists in legally established prohibition of interference into the legal powers and competences of the national supervisory authority;<br><br>- the operational independence of the national supervisory authority should be ensured through the existence of sufficient budgetary and human resources to allow independent exercise of supervisory and advisory functions;<br><br>- the legal statute and structure of the national supervisory authority should ensure the protection of its members against dismissal as a consequence of exercising their supervisory powers;<br><br>- the independence of the national supervisory authority includes the composition of the authority, the | - The independence of the national supervisory authority is explicitly laid down in national legislation;<br><br>- the national supervisory authority is a separate body within the public administration which exercises its supervisory powers independently;<br><br>- the independence of the national supervisory authority is guaranteed by law regulating the procedure for appointing its (chief) representatives; |

| | |
|---|---|
| method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority and the adoption of decisions without being subject to external orders or injunctions;<br><br>- to clearly declare the independent position of the national supervisory authority, Member States should be or become Party to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 8 November 2001. | |
| *2.2.* **National Supervisory Authority – powers and competences (inspections)** | |
| - The national supervisory authority is granted powers and competences (on the basis of relevant national legislation) to exercise effective independent supervision of data processing in all national bodies involved with data processing in the SIS and accessing the system;<br><br>- an inspection policy (plan) with regard to investigation of the SIS should be developed and implemented within the national supervisory authority;<br><br>- the national supervisory authority should have access to N.SIS (including access in situ and access to log files) and the competence to require and receive documentation relevant to the object of the inspection (ad hoc complaint or general supervision);<br><br>- the national supervisory authority should clearly state conclusions and recommendations for acknowledgment or, if necessary, improvement of the data processing;<br><br>- the national supervisory authority should have the competence to take | - All powers and competences of the national supervisory authority are clearly defined by law;<br><br>- the national supervisory authority carries out regular inspections related to SIS; these inspections are based on ad hoc complaints as well as an annual action plan;<br><br>- the inspection policy (plan) is based on a thorough assessment of the data-processing activities of the bodies responsible for SIS data processing; the national supervisory authority assesses all risks, covering all aspects of the SIS data processing;<br><br>- the inspections focus not only on N.SIS, but also on authorities entitled to access the SIS data or input data; use of the SIS is examined also in practice e.g. at external Schengen borders, local police stations, consulates etc.;<br><br>- the national supervisory authority regularly carries out inspections on the basis of analysis of log-files;<br><br>- if not provided for specifically by national law, there is a formal understanding (e.g. |

| | |
|---|---|
| such an action so any change necessary in order to meet requirements of the provisions on data protection in the SIS is implemented;<br><br>- the national supervisory authority should carry out inspections regularly and not only in response to complaints;<br><br>- in the case of a federal state, formal agreements should be concluded between the federal supervisory authority and the regional authorities regarding cooperation and coordinated approach to inspections of the SIS. | exchange of letters, memorandum between authorities concerned) agreed between the national supervisory authority and authorities processing personal data in the SIS, aimed at formalising the arrangements for communications with the national supervisory authority and the formalities of inspections;<br><br>- a request by the national supervisory authority concerning necessary changes in data processing in the SIS should be either legally binding or vested with other forms of effective powers of intervention in accordance with Data Protection Directive 95/46/EC.<br><br>- the national supervisory authority organises follow-up visits to these inspections to verify that its previous opinions/ recommendations have been implemented and identified errors have been corrected;<br><br>- the national supervisory authority has access to the N.SIS in situ via qualified personnel of the data controller or (IT) experts of the national supervisory authority;<br><br>- in a federal state, regular consultations take place between the federal supervisory authority and regional authorities; close relations are established between all authorities. |
| *2.3.* **National Supervisory Authority - organisational structure, budget, staff** | |
| - The national supervisory authority has all necessary human, financial and logistical resources to exercise its powers;<br><br>- besides the top management functions, the national supervisory authority should have on its staff lawyers, IT | - The national supervisory authority is (where possible) structured according to its tasks and competences in different units for management, administration, auditing, supervisory tasks, legal tasks, information tasks and training;<br><br>- the national supervisory authority has an |

| | |
|---|---|
| specialists, information officers and administrative and support personnel;<br><br>- the national supervisory authority should be granted the right to decide for itself how it spends its budget;<br><br>- if resources are not sufficient to exercise the competences of the national supervisory authority independently, a procedure should be established to enable the authority to request improvements; | independent budgetary status within the state budget;<br><br>- the budget of the national supervisory authority reflects specific tasks related to its competences vis-à-vis SIS (e.g. costs of inspections and of public awareness activities);<br><br>- the national supervisory authority develops a training module for its staff dealing with SIS-related issues. |
| **3. RIGHTS OF DATA SUBJECTS**<br>*Art. 109, 110, 111, 114 sec. 2 and 116 CISA* | |
| *3.1.* **General provisions** | |
| - The rights of the data subjects should be governed by national legislation establishing clear rules and procedures available to all parties involved;<br><br>- these rights (including the right to remedy) are exercised in accordance with national legislation in any Member State, irrespective of the citizenship of the data subject;<br><br>- the data subject request has to be dealt without undue delay;<br><br>- any charge related to these rights should not exceed a reasonable fee;<br><br>- arrangements for dealing with requests from data subjects located abroad should be developed including a | - There is a guideline for data subjects explaining how to exercise their rights. This guideline is available on the website of the national supervisory authority as well as of the authorities responsible for N.SIS. Such a guideline is also available in other languages of the participating Schengen States; guidelines created under the Joint Supervisory Authority might be used;<br><br>- standard forms or letters for exercising the rights of the data subjects are available on the website of the national supervisory authority as well as of the authorities responsible for N.SIS;<br><br>- the rights are exercised free of charge;<br><br>- a contact list of the competent authorities |

| | |
|---|---|
| procedure for confirming the identity of the data subject and the authenticity of the request;<br><br>- in the case of a federal state, procedural arrangements between the federal level and the regional level should be developed on the handling of requests and complaints of data subjects. | responsible for dealing with requests concerning the rights of data subjects is maintained and made public;<br><br>- the national supervisory authority can (in cooperation with other national supervisory authorities) provide information and advice not only on the rights of data subjects but also on basic aspects of procedure in other Member States. |
| *3.2.* **Right of access, right to correction and deletion, right to verification** | |
| - The data subject has the right of access to his/ her personal data processed in the SIS, the right to request correction or deletion of his/her personal data and the right to approach the national supervisory authority to request verification of his/her data in the SIS;<br><br>- when, on the basis of the individual's request, the national supervisory authority has to check the data in the SIS entered by another Member State, this should be carried out in close coordination with the national supervisory authority of that Member State;<br><br>- refusal of the right of access must be based on national legislation and the Schengen Convention and only to the extent necessary for the grounds for refusal;<br><br>- when state security, criminal investigation or the rights of third parties are not jeopardized, the data subject must be granted maximum information;<br><br>- where access/ deletion or correction is refused, the data subject should be able to appeal to the national supervisory authority or to another independent body that has the power to investigate whether the refusal/ processing of such data is | - Data subjects are informed after the expiry of alerts under Art. 99 of the Schengen Convention that data have been collected on them, unless the exception referred to in Article 109(2) applies ;<br><br>- a recording system is established, providing for a statistical overview of all exercised rights to access SIS including their follow-up, and also allowing better insight into the quality of the processed data;<br><br>- each request is dealt with on a case-by-case basis, taking into account all circumstances; the response is in principle not limited to the information that the data have been processed in accordance with law (the processed data are communicated);<br><br>- the national legislation does not limit the frequency of the data subject's requests;<br><br>- a reply to the request is generally given without undue delay, no later than after 30 days. If the alert is issued by another Schengen State and cooperation with that state is necessary, the period may not be longer than 4 months. |

| | |
|---|---|
| well founded;<br><br>- national legislation should not limit the frequency of exercising the rights of data subjects more than "at reasonable intervals";<br><br>- when replying to a request from a data subject, the principle of justice without excessive delay should be respected (e.g. a period longer than 4 months could be generally considered as excessive);<br><br>- if the right of access is exercised directly (by the data controller), the national supervisory authority should request (or be provided with) regular reports on the number of such requests in general, the number of inadmissible requests, the number of refusals of communication of data, the number of cases where there was no alert in the SIS, the number of communications on the content of the alert and the approximate time taken to reply;<br><br>- when a data subject exercising his right of access is a lawful resident in another Member State and is the subject of an SIS alert issued by a Member State under Art. 96 of CISA, it should be verified whether the procedure provided for in Article 25(2) of CISA is observed. | |
| *3.3.* **Remedies** | |
| - The procedure for exercising these rights should be clear and available to all parties involved;<br><br>- decisions of the controller or national supervisory authority can be appealed against by courts (or other authority competent under national law), which can decide whether the data subject shall obtain information, have it corrected or | - A guideline for data subjects on how to exercise this right is available on the websites of the national supervisory authority as well as of the authority responsible for N.SIS;<br><br>- all parties involved are heard by the court. They are formally invited to state their case;<br><br>- when a decision refers to an alert issued by |

| | |
|---|---|
| deleted or obtain compensation in connection with an alert in the SIS concerning him/her;<br><br>- the national legislation should not limit direct execution of a final decision of such court or authority; i.e. for the action required, such as communication of the data, deletion or correction, no further procedure is needed in the state that inserted the alert;<br><br>- Article 111 CISA final decisions must be equally enforced by all Schengen States;<br><br>- procedures should be created for monitoring the execution of final decisions and it should be made possible for national supervisory authorities to check whether these final decisions have been executed. To this end, communication among the corresponding national supervisory authorities is necessary;<br><br>- an individual is not responsible for monitoring the execution of decisions concerning his/ her personal data in another Member State. | another Schengen State, the national data protection authorities will inform each other of the decision and the execution of the decision;<br><br>- final decisions taken under Article 111 by courts are communicated by the authority taking that decision to the national supervisory authority; if such an obligation is not imposed by law, the procedure for communication is agreed between the national supervisory authority and the SIS data controller. |
| **4. SECURITY OF DATA**<br>*Art. 118, 126 and 127 CISA* | |
| - Security measures should be determined on the basis of a risk assessment management process in which the scope and assets of the SIS, the risk to it, and the counter-measures required are identified through a system-specific requirement statement (SSRS);<br><br>- the implementation of security measures should comply with accepted international standards;<br><br>- security of data consists in access to premises, access to the SIS as well as regular checking of all measures and | - Random checks of the log files are performed by the national supervisory authority as well as by the data controller, in order to discover any possible misuse of the SIS; at least one check is carried out each year;<br><br>- the national supervisory authority organises regular inspections of the N.SIS and SIRENE premises;<br><br>- the data controller uses a (software) tool allowing them to analyse inappropriate entry into the system; |

| | |
|---|---|
| their implementation in everyday practise;<br><br>- a technical solution must be available with a single central implementation of the SIS;<br><br>- all queries must be logged;<br><br>- there should be clear and specific rules for access to the SIS data;<br><br>- a list of persons having access to the SIS and to log files should regularly be examined to verify that the purpose and extent of the access are appropriate and clearly defined;<br><br>- an adequate system (automated or manual) for searching the SIS log files to identify any misuse is needed;<br><br>- a procedure should be introduced to ensure that personal data in the log files are deleted within the required time limit;<br><br>- encrypted passwords should be used in the authentication procedure;<br><br>- compliance with all security rules should be checked regularly by the data controller as well as by the national supervisory authority. | - a two-factor authentication system is introduced (certificate and encryption keys stored on a smart card, together with a personal identification number; the card and PIN have to be presented in order to access the SIS). |
| **5. DATA PROTECTION IN RELATION TO VISA ISSUANCE** | |
| *5.1.* **Data transfer, access to the SIS and security** | |
| - All competent authorities and services responsible for issuing visas, examining visa applications, issuing residence permits or administering legislation on aliens in the context of the application of the provisions of the Schengen Convention relating to the movement of | .<br><br>- Access to the SIS is only possible by means of a personal user ID and a password. There are rules on regular changing of passwords, prohibition of communicating user IDs and passwords to other persons and on the safe storage of user IDs and passwords; |

| | |
|---|---|
| persons should benefit from online access to SIS provided through a secured communication link;<br><br>- if access to the SIS is provided off-line (e.g. CD-ROM), security features — in particular during transportation — must be provided; in addition, old CD-ROMs must be destroyed;<br><br>- fall-back procedures should be prepared in case of unavailability of the system in consulates, so that the visa-issuing procedure is not affected;<br><br>- suitable measures should be implemented for security and protection of the building/ premises;<br><br>- the organisation of access and use of the SIS by diplomatic and/or local staff should be properly regulated by formal directives;<br><br>- access to the SIS must be reserved exclusively to duly authorised staff of consulates; local staff should be restricted to read-only access;<br><br>- consular officials can only query the system when such a query is linked to a valid visa application;<br><br>- local staff can execute only activities that correspond to the level of authorisation assigned to the local staff by the consul;<br><br>- a written procedure for granting authorisations should be introduced;<br><br>- a routine should be set up whereby the list of persons authorized in consulates is kept up to date and cross-checked with the logs;<br><br>- staff of consulates receive regular training on the implementation of data protection requirements; | - local staff at diplomatic missions only have information to the extent of "hit/no hit";<br><br>- regular training on data protection aspects of visa issuance is introduced;<br><br>- main rooms are physically secured as follows:<br>  - security alarm at the processing area, entrance and exit areas and windows;<br>  - CCTV monitoring 24/7;<br>  - access control system (cards, biometrics);<br>  - automatic fire and flood detectors;<br>  - complete inaccessibility after working hours;<br>  - alternatives available in case of power black-out;<br><br>- the physical & system security of the back-up system is as follows:<br>  - different secure building;<br>  - access control system ( cards, biometrics);<br>  - CCTV monitoring;<br>  - security alarm;<br>  - computer terminals for access to the system;<br>  - log files and log history;<br>  - alternatives available in case of power black-out;<br>  - periodical checks by the system administrator;<br><br>- the security of the building/ premises might include:<br>  - security guard at the entrance;<br>  - protection by an alarm system;<br>  - monitoring by CCTV 24/7;<br>  - automatic fire, flood & smoke detectors;<br>  - protected access to the building (access cards, security locks or biometric system);<br>  - a system of message notification (alert) using SMS or email to the system administrator in case of violation of the system is introduced; |

| | |
|---|---|
| - the main rooms where visa issuance is organised are physically protected against abuse from inside and outside;<br><br>- if visa issuance is a matter that concerns several public authorities, cooperation between these authorities should be governed by a coordination platform where the national supervisory authority is present. | - security checks are carried out on visitors and their belongings;<br>- after working hours the rooms are locked and inaccessible;<br>- the system of authorisation applies to every member of the staff, including cleaning staff. |
| *5.2.* **Inspections in the field of visa issuance** | |
| - An inspection policy (plan) should be developed and implemented, including inspections of consulates aimed at conformity with data protection and data security rules;<br><br>- the national supervisory authority should check the procedures applied when off-line access to SIS is provided (especially when CD-ROMs are used). | - Inspections in the field of visa issuance are a regular activity of the national supervisory authority;<br><br>- the national supervisory authority verifies to what extent proper access and log rules have been established at all consulates and how these procedures are maintained. |
| *5.3.* **Rights of visa applicants** | |
| - The consulates should provide clear instructions that every applicant has the right to access his/her personal data in the SIS, the right to have the data corrected or deleted and the right to approach the national supervisory authority;<br><br>- the visa applicant should be informed of the procedure for exercising his/ her rights to have the data corrected or deleted, including the related remedies established in national law in accordance with the Common Consular Instructions on Visas for Diplomatic Missions and Consular Posts (i.e. at the expressed request of the visa applicant, the | - The websites of consulates contain special information about rights of data subjects including rights of (refused) visa applicants (rights of access to the SIS, rights to appeal etc.);<br><br>- notification of refusal of the visa contains information on rules for exercising the right to access the SIS;<br><br>- leaflets providing general information on how to exercise the rights of the data subject (visa applicant) are available in consulates or on websites in several languages. |

| | |
|---|---|
| consulate provides information on the rights and the procedure; the applicant should also be informed that his/her data may be stored in national databases accessible to the relevant authorities in the Member States);<br><br>- any foreigner should be able to obtain full information on how to exercise his/her right with regard to the SIS at a consulate;<br><br>- the national supervisory authority should be involved in providing this information about the rights of visa applicants. | |
| **6. PUBLIC AWARENESS** | |
| - The authorities responsible for N.SIS and the national supervisory authority should take measures to ensure that the public is well informed of the existence of the SIS as well as of its rights in regard to this file;<br><br>- it is of particular importance to provide information on the right of access to data, on the right of correction or deletion of data with reference to the data in the SIS and on the right to ask the national supervisory authority to check data and the use of them; the procedure for exercising these rights should be clearly specified as well;<br><br>- the authorities responsible for N.SIS and the national supervisory authority should organise permanent information facilities (websites etc.) informing the public about objectives, data, authorities and all rights of data subjects with regard to the SIS (websites are among the most vital media; leaflets containing general information might be considered for most exposed places like consulates or airports); | - The authorities responsible for N.SIS and the national supervisory authority carry out a permanent information campaign; information on the national and international legislation, a general description of the SIS and all necessary information for the public on how to exercise their rights as data subjects and on the functioning of the national supervisory authority itself, contacts etc. are available;<br><br>- public information is updated to keep up with new developments;<br><br>- all authorities accessing the SIS are involved in the information campaign (e.g. coordination on preparation of leaflets or forms, interconnection of all relevant websites including the national supervisory authority);<br><br>- helpful aids (such as model letters, forms, complaints procedures, guidelines and FAQ systems) are created and provided on the websites of the authorities responsible for N.SIS and the national supervisory authority in other languages (several/ all) of Schengen |

| | |
|---|---|
| - all authorities responsible for the SIS should provide a clear and unequivocal picture of the legal provisions, at all times and for all users and subjects; mutual cooperation between these authorities and the national supervisory authority is advisable. | States;<br>- information leaflets concerning SIS and the rights of data subjects are available at border crossing points, police stations and consulates;<br>- the national supervisory authority publishes results of investigation reports and activity reports. |
| **7. INTERNATIONAL COOPERATION**<br>*Art. 106 sec. 3, art. 109 and 110, art. 111 sec. 2, art. 114 sec. 2 CISA* | |
| - The national supervisory authority should cooperate with other supervisory authorities to the extent necessary for the performance of their duties;<br>- fixed time limits and a language regime should be agreed when cooperating with other data protection authorities;<br>- if no time limits are applicable or set, the principle "without undue delay" should apply;<br>- when a national supervisory authority is involved in a procedure pursuant to Articles 106, 109 and 110 it should, if the alert is issued by another Schengen State, inform the supervisory authority of that state of its opinion;<br>- when a data subject uses his/her right of access in the State where he/she lives, and if there is a clear indication that his/her data have been exchanged with other Schengen States or organisations (such as Interpol), the data subject may ask the national supervisory authority of the State where the right of access is exercised to assist him. This assistance may include an investigation as to whether data have indeed been exchanged with other Schengen States or | - The national supervisory authority participates in activities organised by the Joint Supervisory Authority or other joint supervisory bodies or with the European Data Protection Supervisor;<br>- requests for cooperation from abroad are answered without undue delay (the interest of the data subject has priority);<br>- communication between the national supervisory authorities is carried on in a language that is likely to be understood on both sides (if only one language is used, English is recommended, or otherwise a language both national supervisory authorities have agreed on);<br>- when the national legislation does not allow formal communication in a foreign language, the authority in question has to provide for a translation suitable for the addressee;<br>- that some materials or information might also be presented to the data subject has to be taken into account when choosing the language regime;<br>- a contact list of the competent authorities responsible for dealing with requests concerning the rights of data subjects is produced and made public; |

| | |
|---|---|
| organisations. If exemptions to the right of access apply in this specific case such an investigation could take place *ex officio*. The national supervisory authority should contact the national supervisory authorities of those States or organisations with a request to start a procedure for the right of access. The requested national supervisory authorities should treat such a request as a request for access according to their national law and report their decision to the requesting national supervisory authority. The data subject should be informed of the results;<br><br>- if a procedure in a Schengen State results in a final decision of a court, and this decision (also) includes an obligation to correct or delete data transmitted by another State or organisation, the transmitting State should be informed of this decision. Those responsible for the processing of these data and the supervising authority in the transmitting State should be informed that the court decision includes an order to correct or delete data. If a national supervisory authority is involved in such a case, or when it is informed about the outcome, it should inform the national supervisory authority of the transmitting State of the court decision. In return, a national supervisory authority receiving such information should inform the sending authority whether it resulted in correction or deletion of data. | - a specific form may be used to facilitate cooperation between national supervisory authorities;<br><br>- if Schengen States cannot reach an agreement as to whether data in the SIS must be corrected or deleted (art. 106 sec. 3 CISA), the national supervisory authority involved in the case contacts the national supervisory authority of the other Member State;<br><br>- when, due to different national legislation, only one national supervisory authority is involved in dealing with the request for access (on the basis of indirect access or when it presents its opinion at the request of the body responsible for dealing with the request), it informs the national supervisory authority in the other Schengen State of its opinion (art. 109 CISA);<br><br>- where appropriate, the national supervisory authority may be asked to forward a request for an opinion concerning the right to access applied in other Schengen State (art. 109 CISA);<br><br>- when cooperation between national supervisory authorities is needed in dealing with a request for correction or deletion (art. 110 CISA), the principles laid down in Art. 114 sec. 2 CISA apply similarly;<br><br>- if the national supervisory authority is informed of or involved in a judicial procedure in accordance with Art. 111 CISA concerning an alert inserted in another Schengen State, it informs the national supervisory authority of that state (where appropriate, including own opinion); when a check has to be carried out, cooperation is effected in accordance with Art. 114 sec. 2 CISA;<br><br>- the national supervisory authority forwards the court decision concerning an alert inserted by another Schengen State to the national supervisory authority of that state; |

| | |
|---|---|
| | - the national supervisory authority monitors how final court decisions (incl. decisions issued in another Member State) concerning the alerts inserted in the Schengen State concerned are followed up. |
| **8. THE USE OF ALERTS**<br>*Art. 96, 97, 98, 99 CISA* | |
| **8.1 Article 96** | |
| - The appropriate national authorities responsible for Article 96 alerts should inspect these alerts on a regular basis;<br><br>- national supervisory authorities should further invest in developing a joint model of inspection to be used to inspect the alerts in the SIS;<br><br>- 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;<br><br>- 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 these data are checked;<br><br>- measures should be implemented or further developed to prevent Article 96 alerts on nationals of EU Member States. | - 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, cannot be seen as a procedure to ensure that data are accurate, up to date and lawful. |
| **8.2 Article 97** | |
| - Each Schengen State should have formal written procedures in place for all authorities involved with entering Article 97 alerts.<br><br>- In cases where various authorities are | |

| | |
|---|---|
| involved with entering Article 97 alerts, the procedures should be consistent and applied in a uniform manner.<br><br>- When data on a person who is the subject of an alert are to be communicated, the consent of that person is required. The consent of a person who is the subject of an alert should be in writing or at least written proof should be available.<br><br>- In cases where consent is refused, this should always be in writing or recorded officially.<br><br>- Data on minors should always be controlled by automatic means and formal procedures in order to prevent them remaining the subject of an alert after they come of age.<br><br>- The M form should be used by each Schengen State.<br><br>- Each Schengen State should check whether the national authorities having access to Article 97 alerts are considered to be authorities as referred to in Article 101(1) CISA. | |
| **8.3 Article 98** | |
| - In each Schengen State formal written procedures should be in place for all authorities involved with entering Article 98 alerts.<br><br>- In cases where various authorities are involved with entering Article 98 alerts, the procedures should be consistent and applied in a uniform manner.<br><br>- Compliance of the review of data and the retention periods with Article 112 and Article 112A CISA should be improved.<br><br>- The G form should be used by each Schengen State. | |

| | |
|---|---|
| - Each Schengen State should check whether the national authorities having access to Article 98 alerts are considered to be authorities as referred to in Article 101(1) CISA. | |
| **8.4 Article 99** | |
| - Authorities responsible for Article 99 alerts should develop formal and written structured procedures to ensure that Article 99 data are accurate, up to date and lawful;<br><br>- the appropriate national authorities responsible for Article 99 alerts should check and inspect these alerts every six months. Additional guidelines should be set out;<br><br>- where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organized and interlinked in such a way that data are kept accurate, up to date and lawful, and that the data are checked;<br><br>- an alert concerning contact persons is not permissible in view of the wording of Article 99(2);<br><br>- national supervisory authorities should inspect the Article 99 alerts periodically. | - The SIRENE Manual, which sets out the rules and procedures governing bilateral or multilateral exchange of supplementary information, cannot be seen as a procedure to ensure that data are accurate, up to date and lawful. |