THE SCHENGEN INFORMATION SYSTEM

A GUIDE FOR EXERCISING THE RIGHT OF ACCESS

This guide has been compiled by
the Joint Supervisory Authority
of Schengen

Address: Data Protection Secretariat
Council of the European Union
175, Rue de la Loi (00FL59)
B-1048 BRUSSELS
tel:+32(0)22818996

TABLE OF CONTENTS

This Guide describes the arrangements for exercising the right of access to the Schengen Information System (SIS).

While initially intended for data subjects in order to assist them in exercising their right of access, it is meant to be a source of practical information which can also be consulted by anyone with a professional interest in rights of access (data protection authorities, police forces, aliens departments, lawyers, etc.).

The Guide falls into three sections: an outline of the general principles and main definitions relating to the SIS, a description of the procedure for exercising the right of access in each of the countries concerned, and a presentation of some special cases requiring a particular procedure.

I. OUTLINE OF GENERAL PRINCIPLES

I.A The Schengen Information System (SIS)

The Schengen Agreement of 14 June 1985 and its implementing Convention of 19 June 1990 created an area for the free movement of persons by removing checks at internal borders between Member States and establishing the principle of a border control upon entry into a single Schengen territory.

To maintain a satisfactory level of security it was considered necessary, among other measures (strengthening police and judicial cooperation, harmonising visa and asylum policies), to create the Schengen Information System (SIS).

The SIS is a data file shared by all Member States in the Schengen area. It centralises two broad categories of information on, firstly, wanted or missing persons and persons under surveillance and, secondly, stolen or missing vehicles and objects such as, in particular, identity papers, vehicle registration certificates and vehicle number plates.

The following are examples of the data which may be stored in the Schengen Information System:

- persons wanted or under surveillance by the police,
- missing persons or persons who need to be placed under protection, in particular minors,
- persons, not nationals of a Member State of the Schengen area, who are banned from entry into Schengen territory.

The execution of a request is subject to the national law of the Schengen State executing the request. If a measure is not permitted under that national law, the requested Schengen State must inform the reporting Schengen State without delay.

In accordance with data protection principles, all individuals are recognised specific rights by the Schengen Convention .
These are basically:

- the right of access to data relating to them stored in the SIS;
- the right to rectification when data are factually inaccurate or deletion when data have been stored unlawfully;
- the right to ask the national data protection authorities to check data entered in the SIS which concern them and the use made of such data;
- the right to bring proceedings before the courts or competent authorities to correct or delete incorrect data or to obtain compensation.

I.B Right of access

Right of access is the possibility for anyone who so requests to consult the information relating to him stored in a data file as referred to in national law. This is a fundamental principle of data protection which enables data subjects to exercise control over personal data kept by third parties.

This right is expressly provided for in the Schengen Convention of 19 June 1990. Under Article 109 of the Convention anyone has the right to have access to data entered in the Schengen Information System (SIS) which relate to him. This right is accompanied by the right to correction when the data are factually inaccurate or deletion when the data have been stored unlawfully (Article 110).
The right of access must be refused if it could undermine the performance of the legal task specified in the alert, or in order to protect the rights and freedoms of others. It must be refused in any event during the period of validity of an alert for the purpose of discreet surveillance (Article 109 (2) of the Convention).

Anyone exercising his right of access may apply to the competent authorities in the Schengen [1] country of his choice. This choice is possible because all national databases (N.SIS) are identical to the central system (C.SIS) in Strasbourg (see Article 92(2) of the Convention). The right of access therefore pertains to identical data regardless of the State to which the request is addressed.

However, the right of access is exercised in accordance with the law of the State addressed. The rules of procedure differ from one country to another, in that there are currently two types of system governing the right of access to police data files – and thus the SIS. In some countries the right of access is direct, in others it is indirect.

Anyone who so wishes may obtain information about the system which is applicable to the right of access and correction from the national data protection authority in the respective Schengen State.

I.B.1 Right of direct access

In this case the person concerned applies directly to the authorities handling the data (police, *gendarmerie*, customs, etc.). If national law permits, the applicant may be sent the information relating to him.

[1] Belgium, Czech Republic, Hungary, Malta, Lithuania, Latvia, Netherlands, Luxembourg, France, Germany, Italy, Portugal, Spain, Austria, Greece, Denmark, Slovenia, Slovakia, Poland, Sweden, Switzerland, Finland, Norway and Iceland (situation at October 2009).

I.B.2 Right of indirect access

In this case the person sends his request for access to the national data protection agency of the State to which the request is addressed. The data stored in the SIS is verified by the data protection agency in the same way as for police files relating to national security, defence or public security.

Arrangements for disclosing data vary from country to country (see below) and can be extremely limited in some cases.

I.C Principle of the correction or deletion of data

Under the Schengen Convention only the State which issues an alert entered in the SIS may alter or delete it (Article 106).

When a country which applies a right of direct access receives a request for access to an alert which it did not itself issue, that State must give the issuing country the opportunity to state its position as to the possibility of disclosing the data to the applicant.

In the case of a country which applies a right of indirect access, the national data protection agencies must cooperate closely on the basis of Article 114(2) of the Schengen Convention (see below).

II. DESCRIPTION OF THE PROCEDURE FOR RIGHT OF ACCESS IN EACH COUNTRY IN THE SCHENGEN AREA

The procedures specific to each country applying the Schengen acquis which are to be followed by persons wishing to exercise their right of access are described in the national fact sheets in chapters IV-XXVII.

Special situations requiring a particular procedure:

III.A Cooperation between national data protection agencies:

When a person sends a request for access to data relating to him to the national data protection authority of one of the Member States in the Schengen area and it transpires upon verification of the data that they were entered by another Schengen State, the supervisory authorities of both States concerned – i.e. the State which received the request and the State which issued the alert – must work in close cooperation.

Given the large number of requests for access involving more than one State and the possible consequences for individual freedoms, in particular the freedom of movement, of an alert in the SIS, efficient and swift cooperation between the supervisory authorities is of the essence. The following principles should apply with due regard to national law:

– A national supervisory authority which receives a request for access must, when the personal data were entered by another State, act in close cooperation with the national supervisory authority of that other State.
  Under no circumstances does a request for cooperation relieve the supervisory authority initially addressed of responsibility.

– The supervisory authority initially addressed must supply the requested authority with all the information in its possession which may be of use in making checks. The requested national supervisory authority must exercise due diligence when conducting the requested checks.

In particular, the supervisory authority must verify whether the alert in the SIS is well-founded, which sometimes involves extending checks to data stored in national files.

– Special priority must be given to processing these requests to avoid excessive delay in replying to the applicant.

If the national law applicable allows the applicant to exercise his right of access directly by contacting the authorities handling the national files, he must be informed of this possibility without delay.

– Once the checks have been completed, the requested supervisory authority sends the supervisory authority initially addressed all the information gathered in the course of its investigations and gives an opinion. In that opinion, the national supervisory authority informs the requesting national supervisory authority of the implications of its national law for rights of access. It may indicate what the decision on the request for access would be under its national law. If it applies direct access, whereas the requesting authority applies indirect access, it will specify whether it agrees to the information being disclosed to the applicant.

III.B Recording of aliases

It often occurs that an SIS alert is issued for a person whose identity has been stolen (e.g. following the theft and use of his identity papers by a third party). The wanted person is recorded under the various identities that he may assume.

SIS alerts for persons whose identities have been stolen pose serious legal and practical problems.

The SIS contains an alert for an identity which corresponds neither in law nor in fact to a person meeting any of the criteria laid down in Articles 95 to 100 of the Schengen Convention. Such alerts are contrary to the principles that data must be relevant and accurate, which are essential elements of data protection.

Moreover, the experience of national supervisory authorities shows that those whose identities have been stolen may be placed in an extremely disadvantageous situation and have great difficulty in asserting their rights.

Without prejudice to the technical solutions eventually envisaged, the following principles should be applied in processing requests for access from persons whose identities have been stolen:

– Given the obligation incumbent on the States participating in the SIS to guarantee that the data entered is accurate and up-to-date, the storing of alerts on persons whose identities have been stolen can be permitted in only a very limited number of cases, i.e. only where the seriousness of the case, under the conditions as mentioned in Article 95-100, warrants the processing of these data.

  The rights of the person whose identity has been stolen – in particular the right to request deletion of an alert prejudicial to him – must be weighed against the risks of deletion.

– When a person whose identity has been stolen exercises the right of access to the data, the State that issued the alert should accede to a request for deletion of the alert with the utmost speed in most cases, particularly where the alert was issued under Article 96 and not Article 95, for instance.

– Finally, it may happen that a person whose identity is entered in the SIS as an "established identity" maintains that his name has been stolen and used for fraudulent purposes. This delicate situation may arise when the perpetrator of the offence has been apprehended and has claimed the identity of the victim of the identity theft. The Schengen JSA believes that in such cases the person who considers that he has been a victim of identity theft must be able to use every possible means to prove that he did not commit the offence of which he is accused and to assert his rights.

III.C Alert for an alien holding a residence permit issued by a Member State

Article 25(2) of the Schengen Convention provides for the following procedure in such cases:
"Where it emerges that an alert for the purposes of refusing entry has been issued for an alien who holds a valid residence permit issued by one of the Contracting Parties, the Contracting Party issuing the alert shall consult the Party which issued the residence permit in order to determine whether there are sufficient reasons for withdrawing the residence permit.

If the residence permit is not withdrawn, the Contracting Party issuing the alert shall withdraw the alert but may nevertheless put the alien in question on its national list of alerts."

It may then happen that a foreign national is the subject of an SIS alert issued by a Member State in the Schengen area under Article 96 of the Schengen Convention although he is lawfully resident in another Member State.

This situation seems illogical, since it should not be possible for a person to be resident in the territory of a Member State in the Schengen area while at the same time being posted in the SIS as an "undesirable alien" in the Schengen area.

In such circumstances it is important that when any data protection agency discovers that a person exercising his right of access to the SIS is in the situation described above, it verifies whether the procedure provided for in Article 25(2) of the Schengen Convention has been observed, usually leading to the deletion of the alert for the person concerned. If the country which issued the permit considers that there is no reason to withdraw a lawfully issued residence permit, the alert must automatically be deleted from the SIS. The Convention allows the State which issued the alert no powers of discretion whatsoever on that point.

An examination of this question by the JSA revealed that the procedure is not systematically applied and that it may prove to be extremely lengthy for the person concerned. Moreover, it appears that Member States believe that they do have powers of discretion as to whether it is necessary to delete an alert on the basis of Article 25(2) of the Schengen Convention.

In the light of the above, data protection agencies should apply the following principles:

– check whether a person who is the subject of an alert in the SIS is in possession of a valid residence permit issued by a Member State in the Schengen area,
– if so, remind the authorities concerned that deletion of the alert is automatic (exceptions apart) and urge that the data be swiftly deleted from the SIS.

IV. AUSTRIA

1. Nature of right of access (direct, indirect or mixed right of access)

In Austria, the right to information under data protection law is fundamentally direct, i.e. requests for information must be addressed to and answered by the party responsible for processing the data (known as the "*Auftraggeber*" ("principal") in Austria). This rule applies in general under Austrian data protection law and would also apply in particular to information in the SIS concerning alerts pursuant to Articles 95 to 100 of the Schengen Convention.

2. Contact details of the body to which requests for access should be addressed

Requests for information must be addressed to the police authority (as principal) from which the person concerned wishes to know if it has processed data concerning him or her.

3. Formalities for the request: information and documents to be supplied – possible costs

Pursuant to §26 of the *Datenschutzgesetz (DSG) 2000* (Data Protection Act 2000) the principal must provide the person concerned with information:

– where requested in writing by the person concerned (and orally with the principal's consent), and
– if the person concerned proves his or her identity in due form (i.e. a copy of an identity card).

The information must include:

– the data processed,
– available information on its source,
– all recipients or groups of recipients of data transmissions,
– the purpose of use of the data,
– the legal basis, in easily understandable terms,
– at the request of the person concerned, the names and addresses of any service providers processing the data.

Information must not be given:

- if necessary to protect the person concerned for special reasons,
- if overriding, legitimate interests of the principal or a third party constitute an impediment,
- if overriding public interests constitute an impediment to disclosure of the information given the necessity of:
  - protecting constitutional institutions of the Austrian Republic,
  - ensuring that the Federal armed forces are ready for action,
  - protecting the interests of comprehensive defence of the nation,
  - protecting important foreign-policy, economic or financial interests of the Austrian Republic or the European Union, or
  - anticipating, preventing or prosecuting crime.

If disclosure has to be refused in order to protect public interests in the field of law enforcement, the remark that "none of the data relating to the data subject which comes under the obligation to provide information has been used" (paragraph 5) must be indicated in all cases in which no information is given (including where no data has actually been used).
Refusals to provide information are subject to verification by the *Datenschutzkommission* (Data Protection Commission) and to a special appeals procedure.
Information may not be provided if the person concerned has failed to cooperate in the course of the information procedure or has failed to pay the legally requested fee.

The person concerned must cooperate with reasonable questioning in the course of the information procedure.
Within eight weeks the principal must supply the information or give written reasons for not supplying it in part or in full.
Information is supplied free of charge when it concerns an up-to-date database and when the person concerned has not already made the same request in the same year.
In all other cases a flat rate of EUR 18,89 may be charged, which may be varied if higher expenses are actually incurred. If disclosure of the information results in a correction, the fee must be reimbursed.

4. Contact details of the national data protection agency, and its possible role

Datenschutzkommission
Hohenstaufengasse 3
A - 1010 Vienna
Tel.: +43 1 531 15/2525
Fax: +43 1 531 15/2690
E-mail: dsk@dsk.gv.at.

If the police authority fails to meet the eight week deadline, i.e. if no reply has been received, or if notification is given that none of the data relating to the data subject which comes under the obligation to provide information has been processed, the matter may be referred to the Data Protection Commission pursuant to §31(1) and (4) of the Data Protection Act 2000.

If, in an appeal pursuant to §31(4) of the Data Protection Act 2000, the principal pleads the necessity for secrecy in the overriding public interest, the Data Protection Commission must verify whether secrecy was necessary and must order disclosure of the data if secrecy towards the person concerned was not warranted.
The authority may, however, appeal to the *Verwaltungsgerichtshof* (Higher Administrative Court). Otherwise the Data Protection Commission's order must be followed within eight weeks, failing which the Data Protection Commission itself may disclose the data to the person concerned.

5. References of the main national laws that apply

§26 of the Data Protection Act 2000 (DSG 2000), *BGBl.* (Federal Law Gazette) I, No 165/1999.

§26 (1) The principal must supply the data subject with information on data processed in respect of him or her when the data subject so demands in writing and proves his or her identity in due form. With the consent of the principal, requests for information may also be made orally. The information supplied must include the data processed, available information regarding its source, any recipients or groups of recipients of data transmissions, the purpose of use of the data and the legal bases therefore in easily understandable terms. At the request of the data subject, he or she must be supplied with the names and addresses of service providers processing his or her data. With the consent of the data subject, information may be supplied orally instead of in writing, with the option of inspection and a copy or photocopy.

(2) Information must not be supplied where necessary for special reasons in order to protect the data subject or where overriding, legitimate interests of the principal or a third party, in particular overriding public interests, constitute an impediment to the disclosure of information. Such overriding public interests may arise from the necessity of:

1. protecting constitutional institutions of the Austrian Republic, or
2. ensuring that the Federal armed forces are ready for action, or
3. protecting the interests of comprehensive defence of the nation, or
4. protecting important foreign-policy, economic or financial interests of the Austrian Republic or of the European Union, or
5. anticipating, preventing or prosecuting crime.

The admissibility of any refusal to provide information on the grounds in Nos 1 to 5 is subject to verification by the Data Protection Commission pursuant to §30(3) and to the special appeals procedure before the Data Protection Commission pursuant to §31(4).

(3) The data subject must cooperate with reasonable questioning in the course of the information procedure in order to avoid unwarranted and disproportionate work for the principal.

(4) Within eight weeks of receipt of the request either the information must be supplied or the reasons for not supplying it in part or in full must be given in writing. Information may also not be provided because the data subject has failed to cooperate with the procedure pursuant to paragraph 3 or to pay the fee.

(5) In areas of law enforcement responsible for the performance of the tasks referred to in paragraph 2, Nos 1 to 5, the following procedure must be followed if necessary to protect public interests which require a refusal to provide information: in all cases in which no information is provided – also if no data is actually being used – instead of substantive grounds it must be indicated that none of the data relating to the data subject which comes under the obligation to provide information has been used. The admissibility of this procedure shall be subject to verification by the Data Protection Commission pursuant to §30(3) and to the special appeals procedure before the Data Protection Commission pursuant to §31(4).

(6) Information must be supplied free of charge if it concerns the up-to-date content of a data file and if the data subject has not previously requested information from the principal in the current year in the same sphere. In all other cases a flat rate of EUR 18,89 may be charged, which may be varied if higher expenses are actually incurred. Any fee paid must be reimbursed notwithstanding any claims for damages if data was illegally used or if the information resulted in a correction.

(7) Once he is aware that a request for information has been made the principal may not destroy data relating to the data subject for a period of four months and, if an appeal is lodged with the Data Protection Commission pursuant to §31, not until the final conclusion of the proceedings.

(8) Where data files are open to inspection by the public by law, the data subject shall have the right to information to the extent to which there is a right to inspect. The procedure for inspection is governed by the more detailed provisions of the laws establishing the public register.

(9) The special provisions of the Criminal Record Act 1968 governing criminal record certificates shall apply to information from the criminal records.

(10) Should a contractor decide autonomously, on the basis of legal provisions, professional ethics, or codes of conduct pursuant to §6(4) to use a data application pursuant to the third sentence of §4, No 4, the data subject may initially address his request for information to the party which ordered establishment of the application. The latter must immediately inform the data subject of the name and address of the autonomous contractor free of charge, if not already known, to enable the data subject to assert his right to information pursuant to paragraph 1 vis-à-vis the latter.

6. Language regime

According to Austrian legislation, **t**he data subject may start the procedure for the right of access in German.

V. BELGIUM

1. Nature of right of access

Anyone has the right to indirect access to any personal data concerning them which has been processed by police authorities. In order to exercise that right a request must be sent to the Privacy Protection Commission.

2. Contact details of the body to which requests for access should be addressed

Commission de la protection de la vie privée
Rue Haute 139>
1000 Bruxelles

Commissie voor de bescherming van de persoonlijke levensfeer
Hoogstraat 139
1000 Brussel
Tel: +32 2 213 85 40
Fax: +32 2 213 85 65
Website: http://www.privacycommission.be http://www.privacycommission.be/
Email: info@privacycommission.be

3. Formalities for the request: information and documents to be supplied

Requests should be submitted to the Commission by dated and signed letter. The letter should contain the surname and first name, date of birth and nationality of the person concerned plus a photocopy of their identity card.

The name of the authority or service concerned and all relevant information relating to the challenged data – nature, circumstances and source of discovery of data and any corrections desired – should be indicated *if known*.

The procedure is free of charge.

4. Expected outcome of requests for access. Content of the information supplied

When it receives a request for indirect access to personal data processed by a police authority the Commission makes the necessary checks with the authority concerned.

Once the checks have been completed the Commission informs the person concerned that they have been carried out. Where appropriate, when data has been processed by a police authority with a view to identity checks, and following consultation of the authority concerned, the Commission sends the person concerned any other information it considers appropriate.

5. References of the main national laws that apply

– The Act of 8 December 1992 relating to the protection of privacy with regard to the processing of personal data, as amended by the Act of 11 December 1998 transposing Directive 95/46/EC of 24 October 1995, in particular Article 13 thereof;

– The Royal Decree of 13 February 2001 implementing the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data, in particular Articles 36 to 46 thereof.

VI. CZECH REPUBLIC

1. Nature of right of access

The data subject has a right of direct access. The data subject should primarily exercise his rights in respect of the SIS vis-a-vis the data controller, i.e. the Police of the Czech Republic.

2. Contact details of the body to which requests for access should be addressed

Police Presidium of the Czech Republic

P. O. Box 62/K-SOU

Strojnická 27

170 89 Prague 7

3. Formalities for the request: information and documents to be supplied – possible costs

Information on how to apply for information on or correction/deletion of the data is available on the web sites of the DPA (www.uoou.cz), including forms that the data subject may use. The web sites of the Police (www.policie.cz) and the Ministry of Interior (http://www.mvcr.cz/eu-schengen.aspx) provide some information, as does the general "European" web site of the Czech republic (www.euroskop.cz).

Any data subject is entitled to send a written request to the Police of the Czech Republic (address given above) asserting his/her right to information on and deletion or correction of his/her data processed in the SIS. Information about the processing of personal data in the SIS is to be revealed only to the data subject concerned (or his/her attorney). The request must contain identification of the applicant – all first name/s, surname, date and place of birth and address. The Police is obliged to answer within 60 days. Exercise of the right of access is free of charge.

4. Contact details of the national data protection agency and its possible role

The Office for Personal Data Protection

Pplk. Sochora 27

170 00 Praha 7

Czech Republic

The Office for Personal Data Protection is competent to review personal data processing within the national part of the SIS at the request of data subjects in cases where there is suspicion of an unlawful procedure or where the controller (the Police of the Czech Republic) has not provided a satisfactory response.

5. Expected outcome of requests for access. Content of the information supplied

The Police should answer whether any personal data concerning the data subject is contained in the SIS, what it is, why it has been entered (for what purpose) and by which authority.

According to Art. 83/4 of the Police Act the Police must not grant the request if this would jeopardize the accomplishment of police tasks in connection with criminal proceedings or national security or endanger legitimate interests of a third person.

6. References of the main national laws that apply

Act No 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts (Art. 12 and 21)

Act No 273/2008 Coll., on the Police of the Czech Republic (Art. 83 and 84)

7. Language regime

The Czech language is the only official language for communication with the Czech authorities. However, the Czech DPA communicates in English as well. The basic information on how to apply for the right of the access on the web site of the Czech DPA is also available in English.

VII. DENMARK

1. Nature of right of access

The data subject has a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access should be addressed to the Police Service, which is the data controller:

Rigspolitiet
Polititorvet 14
DK-1780 København V
Tel.: +45 33 14 88 88

3. Formalities for the request: information and documents to be supplied – possible costs

There are no particular formal requirements for the dispatch of requests.

Requests for access must be answered as soon as possible, and where in exceptional cases an answer cannot be given within 4 weeks, the data controller must inform the applicant accordingly. Such communication must state the reasons why a decision cannot be taken within 4 weeks and when it can be expected to be taken.

Access should in principle be given in writing if the applicant so requests. Where the data subject goes in person to the data controller, it should be established whether the former wants a written reply or an oral explanation of the contents of the data.

Requests for access are free.

4. Contact details of the national data protection agency and its possible role

Datatilsynet
Borgergade 28, 5. sal
DK-1300 København K
Tel.: +45 3319 3200
Fax: +45 3319 3218
E-mail: dt@datatilsynet.dk
www.datatilsynet.dk

Complaints about the Police Service's decision on access may be made to the Data Protection Agency. In processing complaints, the Data Protection Agency examines the case itself to ensure that no data have been entered in a way which conflicts with the rules of the Schengen Convention.

5. Expected outcome of requests for access. Content of the information supplied

Under Section 31(1) of the Act on Processing of Personal Data, the controller (in this case the Police Service) has to inform a person who has submitted a request whether or not data relating to him are being processed. Where such data are being processed, communication must be made to him in an intelligible form about the data that are being processed, the purposes of the processing, the categories of recipients of the data and any available information as to the source of such data.

Under Section 32(1) in conjunction with Section 30(2) of the Act, this does not apply if the data subject's interest in obtaining this information is found to be overridden by vital public interests, including

(1) national security
(2) ……
(3) public security
(4) the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions
(5) …….
(6) ……..

Under Article 95 and Articles 98 to 100 of the Schengen Convention, the aim of entering information in the Schengen Information System is: the arrest of wanted persons, the appearance of persons summoned, the service of a criminal judgment or a summons, discreet surveillance or specific checks on persons and vehicles and the location of objects sought for the purposes of seizure or use as evidence in criminal proceedings.

In relation to these aims, there will be situations where the data subject may not be told whether information has been entered about him under Articles 95 and 98 to 100 of the Convention. The data subject might otherwise be able to take steps which could seriously jeopardise the measures to be implemented as a result of the alert, see also Article 109(2) of the Schengen Convention.

6. References of the main national laws that apply

Act No 429 of 31 May 2000 on Processing of Personal Data.

VIII. FINLAND

1. Nature of right of access

The data subject has a right of direct access.

2. Contact details of the body to which requests for access should be addressed

The request must be made in person to the local district police.

3. Formalities for the request: information and documents to be supplied – possible costs

Applications must be made to the police in person and applicants must at the same time produce proof of identity.

Exercise of the right of inspection is subject to payment only if less than one year has elapsed since the person concerned last exercised that right.

The keeper of the register must, without undue delay, give registered persons an opportunity to consult the information in the register and must provide information when requested in writing.

4. Contact details of the national data protection agency and its possible role

Albertinkatu 25 A
PL 315,
FIN - 00181 Helsinki
Tel.: ++358 (0)10 36 66700
Fax: ++358 (0)10 36 66735
E-mail: tietosuoja@om.fi
Internet: www.tietosuoja.fi

If the police refuses the right to inspect SIS data on the basis of Section 27 of the Law on personal data, a certificate must be produced to that effect and the registered person must be directed to contact the data protection agency. The registered person can thereafter submit the matter for the agency's consideration.

The data protection agency takes binding decisions on matters concerning right of inspection. Appeals against decisions taken by the agency may be lodged with the relevant administrative court and thereafter with the Supreme Administrative Court (Sections 28 and 29 of the Law on personal data).

5. References of the main national laws that apply

Data Protection Act (523/1999)

Police Data Protection Act (761/2003)

IX. FRANCE

1. Nature of right of access

Right of access is mixed.

Access is direct where persons registered in the SIS are:

- persons wanted for family reasons (Article 97 of the Convention),
- minors prohibited from leaving the country (Article 97),
- minors who have run away (Article 97),
- persons referred to or identifiable when there is a stolen vehicle alert (Article 100).

In all other cases, right of access to SIS is indirect. Under Article 39 of the Law of 6 January 1978 on Data Processing, Data Files and Liberties, the National Data-Processing and Liberties Commission appoints one of its members, a magistrate or former magistrate, who is or has been a member of the Council of State, the Supreme Court of Appeal or of the Court of Auditors, to conduct the necessary investigations and to make the appropriate amendments.

2. Contact details of the body to which requests for access should be addressed

Requests concerning any of the four cases mentioned which are entitled to direct access must be sent directly to:

Direction générale de la police nationale
Ministère de l'intérieur
11 rue des Saussaies
F - 75008 Paris
Tel.: +33(0)1.49.27.49.27
Fax: ---
E-mail: ---
Internet: www.interieur.gouv.fr

In all other cases requests for access should be sent to:

Commission nationale de l'informatique et des libertés

8, rue Vivienne – CS 30223
F - 75083 PARIS CEDEX 02
Tel.: ++33 1 53 73 22 22
Fax: ++33 1 53 73 22 00
E-mail: bmonegier@cnil.fr
Internet: www.cnil.fr

3. Formalities for the request: information and documents to be supplied – possible costs

Right of access is exercised on a strictly personal basis. Requests must be presented by the parties concerned themselves (under no circumstances should they be presented by a family member), or by lawyers acting on their instruction.

There are no particular formal requirements. However, the applicant must indicate his name, first name, date and place of birth and attach to his application a legible photocopy of a document proving his identity. Copies of any relevant documents (notification of refusal of a visa based on an SIS alert, a court decision in favour of the applicant such as the annulment of an expulsion order) should also be attached to the request.

The procedure for right of access is free of charge.

4. Contact details of the national data protection agency and its possible role

Commission nationale de l'informatique et des libertés
8, rue Vivienne– CS 30223
F - 75083 PARIS CEDEX 02
Tel.: ++33 1 53 73 22 22
Fax: ++33 1 53 73 22 00
E-mail: bmonegier@cnil.fr
Internet: www.cnil.fr

5. Language regime

The data subject can submit his request in French.

X. GERMANY

1. Nature of right of access

The right of access in Germany is direct. It is exercised directly by application to the authority responsible for recording the data. If he so wishes, the person concerned may exercise his or her right of access through the data protection agency.

2. Contact details of the body to which requests for access should be addressed

Bundeskriminalamt
– SIRENE Büro –
D – 65173 Wiesbaden
Tel.: ++611 551 65 11
Fax: ++611 551 65 31
E-mail: sirenedeutschland@bka.bund.de

3. Formalities for the request: information and documents to be supplied – possible costs

The person concerned should state his or her surname (maiden name where applicable), first name and date of birth so as to avoid any confusion. Apart from that, there are no particular formal requirements, and the procedure is free of charge.

It is within the competence of the responsible authority – the Bundeskriminalamt – to determine details of the further procedure.

4. Contact details of the national data protection agency and its possible role

The national data protection agency may support the person concerned in exercising his or her rights by forwarding the request for information to the body responsible for recording the data, e.g. the *Bundeskriminalamt* (Federal Bureau of Criminal Investigation), or by initiating a data protection inspection of that body on request. The agency's address is:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30
D - 53117 Bonn
Tel.: ++49-228-997799-0
Fax: ++49-228-997799-550
E-mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

If the request concerns an alert pursuant to Article 96 of the Schengen Convention the information is usually disclosed.

If the request concerns an alert pursuant to Article 95 or Article 99 of the Schengen Convention, it may be refused if at least one of the generally valid reasons for denying disclosure of information, which are laid down in § 19(4) of the Federal Data Protection Law, is applicable to the request; i.e. if disclosure of the information would jeopardise the proper performance of the tasks incumbent upon the recording body or pose a threat to public security or law and order, or if the data or the fact that they have been recorded must be kept secret by law or by definition, in particular in the overriding interests of a third party, and the interests of the person concerned in obtaining the information must consequently give way.

If the alert was issued by a foreign authority pursuant to Article 95 of the Schengen Convention the position of the foreign issuing authority pursuant to the third sentence of Article 109(1) must be taken into account. The information is usually provided by the *Bundeskriminalamt* – SIRENE Bureau. If the person concerned has applied to the national data protection agency the information is supplied by the Federal Data Protection Commissioner. The information usually includes the legal basis for the alert, the date it was issued and the probable length of time for which it will be kept, as well as the issuing authority.

5. References of the main national laws that apply

The main national texts to be applied are Article 109 of the Schengen Convention in conjunction with Article 19 of the Federal Data Protection Law or the relevant regulations on the right to information in the laws on data protection at *Länder* level.

6. Language regime

According to the national legislation "(§23 of the Federal Law on administration procedures - "Verwaltungsverfahrensgesetz") the official language is German, but with regard to European Union citizenship, as mentioned in Article 17 ff. EEC Treaty, applications or requests in EU languages other than German are accepted, too.

XI. GREECE

1. Nature of right of access

Under Article 12 of Law 2472/1997 the right of access is direct (applicants submit their requests directly to the SIRENE Bureau). If applicants send their requests to the Personal Data Protection Authority, they are advised to submit them directly to the SIRENE Bureau.

2. Contact details of the body to which requests for access should be addressed

The law stipulates that requests be sent to the SIRENE Bureau, whose full address is:

Ministry of Citizen Protection
Greek Police
International Police Cooperation Division
3d Division SIRENE
Kanellopoulou 4
GR– 101 77 Athens
Tel.: ++301 69 81 957
Fax: ++301 69 98 264/5
E-mail: info@sirene-gr.com
Internet: ---

3. Formalities for the request: information and documents to be supplied – possible costs

Requests must state the applicant's name and forename, father's forename, applicant's full date of birth and nationality. Other particulars, e.g. the applicant's identity number, passport number, address and telephone number and mother's forename are optional. Applicants must provide a photocopy of their passports.

To exercise their right of access under Article 12 of Law 2472/1997 applicants must pay EUR 5 to the data controller (SIRENE Bureau), and they must pay EUR 60 in order to exercise their right to object under Article 13 of that Law and Decision 122 adopted by the Personal Data Protection Authority on 9 October 2001. We should add that, in order to exercise the right of access to SIS, the essentially paltry sum of EUR 5 is never levied and the Greek Data Protection Authority is considering the possibility of formally abolishing it.

4. Contact details of the national data protection agency and its possible role

Contact details of Greece's national personal data protection agency are:

Hellenic Data Protection Authority
Kifisias 1-3, 1st floor
GR – 115 23 Athens
Tel.: ++30 210 6475600
Fax: ++ 301 210 6475628
E-mail: contact@dpa.gr
Internet: www.dpa.gr

The national Personal Data Protection Authority checks that the SIS alert concerning the applicant is lawful and legitimate.

5. Expected outcome of requests for access. Content of the information supplied

If the alert was issued under Article 96 of the Schengen Convention, the applicant will be informed of the data relating to him.

If the alert was issued under Article 95 or Article 99 of the Schengen Convention, the applicant is likely to be refused disclosure of the data. Moreover, in accordance with Article 12(5) of Law 2472/1997, the data will not be disclosed if the processing has been carried out on national security grounds or in the investigation of particularly serious offences. Where an alert under Article 95 of the Schengen Convention has been issued by a foreign authority, the latter's opinion is taken into account when deciding whether to release the data to the applicant.

The information released to the applicant comprises the legal basis for the alert, the date on which it was entered in the SIS, the department which entered the data, and the length of time it is to be stored.

6. References to the main national laws that apply

The applicable provisions are Article 109 of the Schengen Convention and Article 12 (exercise of the right of access) and Article 13 (exercise of the right to object) of Law 2472/1997.

Comment

Where applicants' particulars have been entered in the SIS by the Greek Police, requests to exercise the right of access and the right to object under Articles 12 and 13 of Law 2472/1997 are made directly to the data controller.

As for the language regime, the official language is Greek, however, requests in English are also considered.

XII. HUNGARY

1. Nature of right of access

The right of access can be exercised both directly and indirectly.

2. Contact details of the body to which requests for access should be addressed

The SIRENE Office of the National Police Headquarters
H-1139 Budapest, Teve utca 4-6.
Tel: +36 1 443 5861
e-mail: sirene@nebek.police.hu

The Office of the Parliamentary Commissioner for Data Protection
H-1051 Budapest, Nádor u. 22.
Tel: +36 1 475 7100
e-mail: privacy@obh.hu

A request for access can be made in person at any police station in the territory of Hungary and at any diplomatic mission of the Republic of Hungary. Requests will be forwarded to the SIRENE Office.

3. Formalities for the request: information and documents to be supplied – possible costs

The person concerned must provide credible proof of his/her identity. Requests can be submitted in Hungarian, English, German or French. The information must be given in writing within the shortest possible time, but not later than within 30 days of the lodging of the request. The request can be made free of charge. If the data subject repeats his/her request during a given calendar year, the costs of providing the information will be charged.

4. Contact details of the national data protection agency and its possible role

The Data Protection Commissioner has the authority to answer requests submitted to him after checking the relevant files in the Schengen Information System. Furthermore, if the data subject has doubts concerning the answer received from the SIRENE Bureau, or if no answer is received from the SIRENE Bureau, he may apply to the Data Protection Commissioner.

5. References to the main national laws that apply

Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest
Act CV of 2007 on Cooperation and Information Exchange in the framework of the Convention Implementing the Schengen Agreement

XIII. ICELAND

1. Nature of right of access

The right of access to information is direct.

2. Contact details of the body to which requests for access should be addressed

Applications should be addressed to the Sirene Bureau in Iceland, which is run by the Commissioner of the Icelandic National Police (CINP).
The CINP's address is:

Ríkislögreglustjóri
Skúlagata 21
IS - 150 Reykjavik
Tel.: ++354 444 2500
Fax: ++354 444 2501
E-mail: rls@rls.is
Internet: www.rls.is

Special application forms can be filled in at local police stations or at the CINP's premises. Decisions on the release of information are taken by the Sirene Bureau.

3. Formalities for the request: information and documents to be supplied – possible costs

The applicant must provide some proof of identity and the application form must be filled in in the presence of a police officer. The applicant may only request access to information regarding himself. However, a legal guardian may request access to information on his ward. Exercise of the right of inspection is free of charge, but each individual will only be granted access once a year, unless special circumstances for more frequent access apply. The Sirene Bureau will consult the DPA (Data Protection Authority) in such cases.

4. Contact details of the national data protection agency and its possible role

In cases where an applicant has received a standard reply: "No information is registered/it is not permitted to disclose registered information" (see point 5), the Sirene Bureau must instruct the applicant that he may appeal against this decision to the Ministry of Justice and Human Rights. The Ministry may seek the DPA's opinion on the Sirene Bureau's decision.

The Ministry of Justice and Human Rights:
Dómsmála- og mannréttindaráduneytid
Skuggasund
IS - 150 Reykjavík
Tel.: ++354 545 9000.
Fax: ++354.552.7340
E-mail: postur@dmr.stjr.is
Internet: www.domsmalaraduneyti.is

The DPA's address is:

Persónuvernd
Rauðarárstígur 10
IS - 105 Reykjavík
Tel.: ++354 510 9600.
Fax: ++354 510.9606
E-mail: postur@personuvernd.is
Internet: www.personuvernd.is

5. Expected outcome of requests for access. Content of the information supplied

The Sirene Bureau must answer all applications without undue delay and no later than a month from receipt of the request. If an applicant is registered, he will be informed of the purpose of and reasons for the registration. In cases where it is necessary to keep the information secret in order to achieve the intended aim of the entry into the information system, or in view of the interests of other persons, or when discreet surveillance is in progress, the data subject does not have the right to be informed of the recorded data. The applicant will be given the same standard reply as an applicant who is not registered, namely "No information is registered/it is not permitted to disclose registered information."

6. References of the main national laws that apply

The main national laws applying are: Act No 16/2000 on the Schengen Information System in Iceland and Regulation No 112/2001 on the Schengen Information System in Iceland.

7. Language regime

Although not stated in law, Icelandic is the language of administration in Iceland. However, if a request in another language is received by an Icelandic authority, it will be answered. If the request is from an individual who is not in a position to understand an answer in Icelandic (e.g. a foreign national who does not have an Icelandic party guarding his interests, e.g. a solicitor), he will be answered in a language that he understands.

XIV. ITALY

1. Nature of right of access

Access may only be exercised directly, by application to the controller, the Public Security Department of the Ministry of the Interior.

2. Contact details of the body to which requests for access should be addressed

Based on the guidance provided by the above Public Security Department, all access and verification requests should be sent to the following address:

Ministero dell'interno
Dipartimento della pubblica sicurezza
Ufficio coordinamento e pianificazione delle forze di polizia
Divisione N.SIS
Via di Torre di Mezza Via 9/121 - 00173 Roma

If the answer to a request is considered to be unsatisfactory, data subjects may lodge a complaint with the Garante per la protezione dei dati personali at the address given below:

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma

Complaints should be sent preferably by post rather than by facsimile, in order to ensure that all the documents are fully readable. They must contain appropriate contact details for the complainant; if possible the latter's postal address, in order to facilitate correspondence.

3. Formalities for the request: information and documents to be supplied – possible costs

No special requirements are to be met in order to lodge the application (which may be sent either by post or by fax) nor is there any fee or tax to be paid. Although there are no express requirements for establishing the applicant's identity in respect of access to the N-SIS in the applicable legislation, in order to expedite the processing of such a complaint, it should be drawn up, if possible, in Italian, English, French or German and **signed by the data subject concerned**, contain a summary description of the grounds on which it is lodged, and be accompanied by a **photocopy of a suitable valid ID pertaining to the data subject**.

4. Expected outcome of requests for access. Content of the information supplied

5. References to the main national laws that apply

The main national laws applicable are as follows:

(a) Law No 388 of 30 September 1993, concerning ratification and implementation of the Schengen Agreement and the relevant implementing Convention (see, in particular, Articles 9, 10, 11 and 12);

(b) Legislative Decree No 196 of 2003.

XV. LATVIA

1. Nature of right of access

Anyone (both nationals and non-nationals of the Member States in the Schengen area) has the right to direct access to personal data held on them in SIS. (This is determined by the Cabinet of Ministers' Regulations No.622 *"Order on how the data subject is to request information and how the data subject is to receive information regarding data stored in the Schengen Information System and the SIRENE information system").* The data subject should be given an answer to his request within one month.

The body competent to rule on any appeal submitted by an individual whose request to view personal data pertaining to him/her has either been refused or unanswered is the State Data Inspectorate, which is also competent to carry out supervision of implementation of the right to correct incorrect data or delete illegal personal data.

2. Contact details of the body to which requests for access should be addressed

The (written) request for direct access should be addressed to the State Police or diplomatic and consular representations of the Republic of Latvia.

State Police
Čiekurkalna 1.linija 1, k-4
Riga, LV-1026
Ph: +371 67075212; fax +371 67371227
e-mail: kanc@vp.gov.lv

Contact information on the diplomatic and consular representations of the Republic of Latvia is available on the website of the Ministry of Foreign Affairs (the link to this information: http://www.mfa.gov.lv/lv/Ministrija/mission).

3. Formalities for the request: information and documents to be supplied

Requests should be submitted to the State Police or to the diplomatic and consular representations of Latvia in person or electronically, by handing in a dated and signed letter. When submitting a request in person, the data subject must to prove his/her identity by presenting an identity document. If the request is submitted electronically, it should be signed with a secure electronic signature.

The request should contain the surname and first name of the data subject; date of birth; personal code (if the person has one); place of birth; state of origin; type (if there is one) and number of the identity document; title of the institution that issued the document; date when the ID document was issued and its expiry date; amount of information requested (information on data subject, information on recipients of data subject information); the way the individual wants to receive the reply (in person at the State Police office or the diplomatic and consular representations of Latvia or indicate the address where the reply should be sent).

The procedure is free of charge.

4. Expected outcome of requests for access. Content of the information supplied

The representatives of the State Police or the diplomatic and consular representations of Latvia, on receiving a request for information from a data subject, verify the identity of the data subject submitting the request and send the request to the sub-unit of the State Police – SIRENE Bureau of Latvia.

The SIRENE Bureau carries out the necessary checks on the request submitted and, within one month, provides the data subject with an answer or a refusal to provide information by sending a reply to the address or the institution indicated by the data subject - the address where the letter should be sent or to the State Police or the diplomatic and consular representations of Latvia.

5. References of the main national laws that apply

- Personal Data Protection Law;
- Law on the Operation of the Schengen Information System;
- Cabinet of Ministers' Regulations No.622 (11.09.2007.) “Order on how the data subject is to request information and how the data subject is to receive information regarding data stored in the Schengen Information System and the SIRENE information system”.

6. Language regime

As for the language regime, all proceedings before Latvian authorities should be in Latvian, according to the Official Language Law of the Republic of Latvia, which also applies to rights of access to the SIS. However, the Law on Petitions (Article 7 section 1 paragraph 4) states that a petition or complaint may be unanswered if the text of the petition cannot be objectively read or understood. The SIRENE Bureau of Latvia has stated that requests in English or Russian are also considered.

XVI. LUXEMBOURG

1. Nature of right of access

Access is indirect, in that the right of access can only be exercised through the supervisory authority.

2. Contact details of the body to which the request for access should be addressed

The Supervisory Authority established under Article 17 of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by the Law of 31 July 2006, the Law of 22 December 2006 and the Law of 27 July 2007.

Parquet Général du Grand-Duché de Luxembourg
(Principal State Prosecutor's Office)
BP 15
L-2010 Luxembourg
Tel.: ++352 47 59 81–331
Fax: ++352 47 05 50
E-mail: parquet.general@mj.etat.lu

3. Formalities for the request: information and documents to be supplied – possible costs

The Law of 2002 lays down no particular requirements for requests.

The procedure is free of charge.

Under Article 17 of the Law of 2002 the supervisory authority will carry out the appropriate verification and investigations and arrange for any necessary rectifications.

4. Expected outcome of requests for access. Content of the information supplied

The supervisory authority will inform the data subject that the processing in question does not contain any data contrary to the treaties, laws and implementing regulations.

Nothing is disclosed with regard to the content of the applicant's data.

5. References to the main national laws that apply

Law of 2 August 2002, as amended, on the Protection of Persons with regard to the Processing of Personal Data.

Regulation of the Grand-Duchy of Luxembourg of 9 August 1993 authorising the establishment and use of a data-bank as the national section of the Schengen Information System (N.SIS) (the Regulation does not cover right of access).

6. Language regime

The data subject may start the procedure for the right of access in one of the following languages:

- Luxembourgish;
- French;
- German;
- English.

XVII. LITHUANIA

1. Nature of right of access (direct, indirect or mixed right of access)

The data subject has a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access, correction or deletion should be addressed to the Ministry of the Interior of the Republic of Lithuania, which is the data controller:

Ministry of the Interior of the Republic of Lithuania
Šventaragio str. 2, LT-01510 Vilnius
Lithuania
Phone +370 5 271 7130, fax +370 5 271 8551
Email korespondencija@vrm.lt

3. Formalities for the request: information and documents to be supplied - possible costs

Requests have to be submitted in writing and signed. They have to include the identity of the person wishing to have access to data concerning him or her, or to have data concerning him or her corrected/deleted (surname(s) and first name(s), personal identification number (if he does not have a personal identification number, date of birth), place of residence, contact details (phone or email address)). The applicant must provide the data controller with a document certifying his or her identity. Exercise of the rights is free of charge.

4. Expected outcome of requests for access. Content of the information supplied

The data subject has the right to obtain information on the sources and the type of personal data that has been collected on him, the purpose of their processing and the data recipients to whom the data are or have been disclosed.

On receiving an enquiry from a data subject concerning the processing of his personal data, the data controller must inform the data subject whether personal data relating to him have been processed, and disclose the requested data no later than within thirty calendar days of the date of the data subject's enquiry.

Where the data subject, after inspecting his personal data, finds that they are incorrect, incomplete and inaccurate or that they have been processed unlawfully and unfairly, and applies to the data controller in writing, the data controller must check the personal data concerned without delay and rectify the incorrect, incomplete and inaccurate personal data and (or) suspend processing of such personal data, except storage. If he finds that personal data are being processed unlawfully and unfairly, the data controller must destroy the personal data collected unlawfully and unfairly or suspend processing of such personal data, except storage, without delay.
The data controller must inform the data subject and the data recipients of the rectification, destruction of personal data or suspension of processing of personal data at the request of the data subject, without delay.

According to paragraph 2 of Article 17 of the Law on Legal Protection of Personal Data the data controller must provide conditions for the data subject to exercise his rights, with the exception of cases provided by law when necessary to ensure:

1) state security or defense;
2) public order, the prevention, investigation, detection and prosecution of criminal offences;
3) important economic or financial interests of the state;
4) prevention, investigation and detection of breaches of official or professional ethics;
5) protection of the rights and freedoms of the data subject or any other persons.

The data subject must be refused information about his personal data where necessary to perform actions regarding the alert or to defend the rights and liberties of third parties. Information concerning personal data must not be disclosed to the data subject within the timeframe valid for alerts on discreet surveillance.
Proper reasons must be given for the data controller's refusal to fulfil the data subject’s request. The data controller must inform the data subject of his refusal to provide the requested data within no more than 30 calendar days of receipt of the data subject’s request.

Article 109(1) of the Schengen Convention of 19 June 1990 provides that the right of persons to have access to data entered in the Schengen Information System which relate to them is to be exercised in accordance with the law of the Contracting Party before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 114(1) is to decide whether information should be communicated and by what procedures. A Contracting Party which has not issued the alert may communicate information concerning such data only if it has previously given the Contracting Party issuing the alert an opportunity to state its position.
Regulations on the Lithuanian National Schengen Information System approved by Order of 17 September 2007 of the Minister of the Interior of the Republic of Lithuania No. 1V-324 provide that in cases where alerts on a data subject have been issued by another Contracting Party, the N.SIS data controller must not disclose information to the data subject concerning personal data on him in the national SIS, until authorization to provide such data has been received from the Contracting Party which issued the alert.

The N.SIS data controller, in response to the data subject's written application for rectification of incorrect, incomplete or inaccurate personal data, destruction of unlawfully processed personal data or suspension of processing operations on personal data, must immediately forward it to the competent institution of the Contracting Party, notifying the data subject accordingly. When the competent institution of the Contracting Party has corrected any incorrect or inaccurate data, updated any incomplete data, destroyed any unlawfully stored data or suspended processing operations on such data, the N.SIS data controller must immediately notify the data subject and the N.SIS data recipients to whom incorrect, inaccurate or incomplete data have been provided.

5. Contact details of the national data protection agency and its possible role

State Data Protection Inspectorate
A.Juozapavičiaus str. 6 / Slucko str. 2, LT-09310 Vilnius
Lithuania
Phone +370 5 279 1445, fax +370 5 261 9494
E-mail: ada@ada.lt
Internet: www.ada.lt

If the data subject is not satisfied with the reply received from the data controller, or the data controller refuses to grant the data subject's request to exercise his/her right to have access to his/her personal data, to request rectification or destruction of his personal data or suspension of further processing of his personal data, or the data controller does not reply to the data subject within 30 calendar days of the date of his application, the data subject may appeal against acts (omissions) by the data controller to the State Data Protection Inspectorate within three months of receipt of the reply from the data controller or within three months of the date when the deadline for replying expires. The data subject can attach documents (the data controller's answer to the data subject's request, etc.), where they exist, substantiating the facts mentioned in the data subject's complaint, in order to ensure that the complaint is investigated efficiently.

After receiving the data subject's complaint, the State Data Protection Inspectorate checks the lawfulness of the personal data processing and takes a decision on the facts described in the complaint.

6. References of the main national laws that apply

The Law on Legal Protection of Personal Data

Regulations on the Lithuanian National Schengen Information System approved by Order of 17 September 2007 of the Minister of the Interior of the Republic of Lithuania No. 1V-324

7. Language regime

Requests for access, correction or deletion must be submitted in the official language of the state (Lithuanian). Requests received in any other language will be investigated according to a general procedure. If the data subject's request is in a language other than the official language of the state, it must be translated into Lithuanian. The reply will be given to the applicant in the official language of the state (Lithuanian).

The language of the complaint investigation procedure is Lithuanian. Where a complaint by a data subject is lodged with the State Data Protection Inspectorate in any other language, it has to be translated into Lithuanian. The decision on the complaint is to be adopted and the reply to the complainant given in the official language of the state (Lithuanian).

XVIII. MALTA

1. Nature of right of access (direct, indirect or mixed right of access)

The data subject has a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access, correction or deletion should be addressed to the competent national authority through the following contact:

Data Protection Officer Insp. Sandro Camilleri
Legal Unit
Police Headquarters
Floriana
Tel: 21224001
Email: sandro.camilleri@gov.mt

3. Formalities for the request

In accordance with Maltese law, the request must be submitted in writing and signed by the data subject. The request must be made in Maltese or English, which are the two official languages recognised by the Maltese Constitution. The reply should be provided in the same language as used by the individual submitting the request. The information should be provided without expense and without excessive delay.

4. Procedure

The Schengen Convention establishes that the right of individuals to request access to their personal data entered in the Schengen Information System (SIS), is to be exercised in accordance with the domestic law of the competent national authority where the request is submitted.

Having submitted a request, an individual is entitled to receive written information in line with the general data protection provisions contained in the Maltese Data Protection Act (Cap 440). Information should be provided in intelligible form about the actual personal data being processed, the source from where information was collected, the purpose of processing, and the possible recipients of information. Refusal or restriction to the right of access may only occur when this is justified for the suppression of criminal offences, or where necessary for the protection of the data

subjects or the freedoms of other individuals.

In the eventuality of a restriction or refusal, the individual is to be informed in writing of such a decision, including reasons for the decision unless such communication could impinge on a legal task of the Police or the rights and freedoms of other individuals.

5. Contact details of the national data protection authority and its possible role

Office of the Data Protection Commissioner
2, Airways House,
High Street
Sliema.
Malta
Tel: +35623287100, fax: +35623287198
Email: commissioner.dataprotection@gov.mt
Website: www.dataprotection.gov.mt

In the case of a restriction or refusal, the individual has a right to file an appeal with the Data Protection Commissioner within thirty days from when the decision is communicated to the individual or when the individual may reasonably be deemed to know about such a decision.

In considering the appeal the Data Protection Commissioner must review the decision and must be satisfied that a refusal or restriction is reasonable and well founded.

6. References to the applicable national legal framework

The applicable legal instruments are the Data Protection Act (Cap 440) and Legal Notice 142 of 2004 regulating the processing of personal data in the Police sector.

XIX. NETHERLANDS

1. Nature of the right of access

The nature of the right of access in the Netherlands is direct. The Police Data Act (Wet politiegegevens) is applicable to the national section of the Schengen Information System (NSIS). A right of access is granted in Article 25 of the Police Data Act. Any individual can submit a written request for access to his personal data in the SIS by sending a request to the Data Protection Officer of the National Police Agency (Korps Landelijke Politiediensten). Within 6 weeks of the request for access a reply should be communicated to the applicant. The reply will contain a communication on the content of the data, unless grounds for refusal of the communication lead to the application of Article 27 of the Police Data Act. Communication may be refused if necessary in the interests of:

a. the proper execution of the police task;

b. significant interests of third parties;

c. the security of the State.

2. Contact details of the body to which requests for access should be addressed

Requests for access to information should be submitted to:

Korps Landelijke Politiediensten
Attention of the data protection officer
Postbus 3016
NL – 2700 KX Zoetermeer
Tel.: ++31-79-345 90 62
Fax: ++31-79-345 90 10

3. Formalities for the request: information and documents to be supplied – possible costs

On receiving a request for information the Data Protection Officer contacts the person concerned regarding arrangements for dealing with the request. A copy of the identity card must be provided. A fee of EUR 4.50 may be charged for dealing with requests.

Requests are examined to establish whether they can be met or whether there are legal grounds for a refusal.

Requests concerning Article 96 alerts will be forwarded to the responsible authority for this category of alerts, the Immigration and Naturalisation Service (IND) of the Ministry of Justice.
Requests concerning all other alerts will be dealt with by the competent (police) authorities.

Once information has been obtained a request may be made for the data to be completed, corrected or deleted.

4. Contact details of the national data protection agency and its possible role

If there is a dispute regarding the processing of the request an application for mediation may be sent to:

College Bescherming Persoonsgegevens
Postbus 93374
NL – 2509 AJ Den Haag
Tel.: ++31(0)708888500
Fax: ++31(0)708888501
E-mail: info@cbpweb.nl
Internet: www.cbpweb.nl

The application must be submitted within 6 weeks of receipt of the information.
Cases in which a request has been refused will be examined free of charge by the College Bescherming Persoonsgegevens (Dutch data protection agency). The College Bescherming Persoonsgegevens can also be asked to examine whether data has been recorded in the Schengen Information System in accordance with the Schengen Convention and the law.
As an alternative, or if mediation by the CBP has failed, an application may be filed with the district court (administrative section) to consider the case and decide as it finds appropriate.

XX. NORWAY

1. Nature of right of access

The right of access is direct.

2. Contact details of the body to which requests for access should be addressed

Kriminalpolitisentralen
(National Criminal Investigation Service NCIS)
PO Box 8163 Dep.
NO-0034 OSLO
Tel.: ++47 23 20 80 00
E-mail:
Fax: + +47 23 20 88 80
Internet: www.kripos.no

3. Formalities for the request: information and documents to be supplied – provide costs

Applications for access must be made in writing and signed. A written reply must be given without undue delay and no later than 30 days from receipt of the request.

4. Contact details of the data protection agency and its possible role

Datatilsynet
PO Box 8177 Dep.
NO-0034 OSLO
Tel.: +47 22 39 69 00
Fax: + 47 22 42 23 50
E-mail: postkasse@datatilsynet.no
Internet: www.datatilsynet.no

5. Expected outcome of requests for access. Content of the information supplied

Applications for access are decided in the first instance by the registration administrator (NCIS). If the application has been made to the registration administrator, it is referred to the authority that ordered the registration with a request for an opinion. If the application has been made to the authority that ordered the registration, this authority forwards it to the registration administrator, accompanied by an opinion.

If access is not granted because the applicant is not registered or because the exclusionary provision of the SIS Act applies (Section 15), alternative grounds must always be given, so that the grounds provided do not indicate that data which cannot be disclosed have been recorded.

6. References of the main national laws that apply

Act relating to the Schengen Information System (LOV 1999-07-16-66)
Regulations to Act No 66 of 16 July 1999 relating to the Schengen Information System (SIS regulations).

XXI. POLAND

1. Nature of right of access

The right of access to information is direct.

2. Contact details of the body to which requests for access should be addressed

According to the Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, Poland's controller of data processed within the Schengen Information System is the Commander-in-Chief of the Police. Requests for access or modification of data should be sent to him.

Address for correspondence:
General Headquarters of the Polish Police (KGP)
Central Technical Authority KSI
02-514 Warsaw
148/150 Puławska Street
Poland

If there is a need for consultation regarding the contents of a request for access to personal data, contact with us is possible by phone or via e-mail:

tel.: +48 (22) 601-53-29
tel.: +48 (22) 601-53-15
e-mail: cot.admin.ksi@policja.gov.pl

3. Formalities for the request: information and documents to be supplied – possible costs

Everyone has the right to obtain comprehensive information regarding personal data concerning them which are processed in data filing systems.

In accordance with Article 32 (5) of the Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2002, No. 101, item 926, with subsequent amendments), the person concerned may exercise his/her right to obtain information *once every six months*.

An application for access is free of charge.

Pursuant to Article 32 (1-5a) of the Act on the Protection of Personal Data the data subject may request the following information regarding the processing of his/her personal data:

- whether the data exist in the system,
- for how long the data have been processed,
- the source of data acquisition,
- how data is made available,
- the purpose and scope of data processing,
- to what extent and to whom the data were made available.

The controller will reply regarding the requested information within 30 days. In order to obtain such information a written request must be submitted in Polish.

The request for information should include:

1. name and surname of the applicant,
2. Polish national identification number - PESEL (where applicable),
3. nationality,
4. date and place of birth,
5. photocopy of an identity document containing a clear image,
6. place of residence (country, city, street and house number/apartment),
7. subject matter of the request,
8. signature of person making the request.

In accordance with Article 32 of the Act of 14 June 1960 on the Code of Administrative Procedure (Journal of Laws of 2000, No. 98, Item 1071, with subsequent amendments), a party may be represented in administrative proceedings by a plenipotentiary, unless the nature of the activities requires action in person. Article 33 of the Code establishes the procedural rules for power of attorney, i.e.:

- the plenipotentiary may be a natural person having legal capacity;
- power of attorney should be notified in writing;
- the plenipotentiary files an original or officially certified copy of the power of attorney.

A lawyer, legal counsel or patent agent may themselves authenticate a copy of the power of attorney granted to him/her.

Refusal to provide information on processed personal data

According to Article 30 of the Act on the Protection of Personal Data the controller may refuse to provide access where this would:

1. result in the disclosure of information constituting a state secret,
2. pose a threat to state security or defence, life and human health or safety and public order,
3. pose a threat to the basic economic or financial interest of the State,
4. result in a substantial breach of personal interests of data subjects or third persons.

The right to correct the data, request the suspension of their processing or removal

The data subject may ask the controller to supplement, update, correct, remove, and temporarily or permanently suspend processing of his/her data. However, the data subject must demonstrate that the data are incomplete, outdated, inaccurate, have been collected in violation of the law or that their processing is no longer necessary to achieve the purpose for which they were collected.

Application proceedings are conducted in accordance with the provisions of the Code of Administrative Procedure.

4. Contact details of the national data protection authority and its possible role

In order to provide an adequate level of legal protection for persons whose data is stored in the Schengen Information System, the General Inspector for Personal Data Protection supervises whether the use of data violates the rights of data subjects. This supervision is exercised in accordance with the laws on personal data protection.

Address for correspondence:
Bureau of the Inspector General for Personal Data Protection (GIODO)
2 Stawki Street
00-193 Warsaw
Poland
tel. +48 (22) 860-73-93
fax +48 (22) 860-70-86
http://www.giodo.gov.pl
kancelaria@giodo.gov.pl

Any person whose data are processed in the Schengen Information System, is entitled to submit a complaint to the Inspector General for Personal Data Protection in relation to the implementation of the provisions on the protection of personal data.

5. References of the main national laws that apply

- Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System,
- Act of 29 August 1997 on the Protection of Personal Data,
- Act of 14 June 1960, Code of Administrative Procedure,
- Act of 7 October 1999 on the Polish Language.

XXII. PORTUGAL

1. Nature of right of access

Citizens have a right of indirect access to SIS data. That right is guaranteed by the National Data Protection Agency.

2. Formalities for the request: information and documents to be supplied – possible costs

Requests must be submitted in writing, using one of the two specific forms, either for the right of access or for the right of rectification or deletion. These forms are available on the DPA website, in Portuguese, English and French versions. The requests may be submitted in person, in the DPA front office, or by post. Applicants must present a document confirming their identity (passport) or send attached to the request an authenticated copy of the passport to have access to the data concerning them. Exercise of the right of access is free of charge.

3. Contact details of the national data protection agency and its possible role

Comissão Nacional de Protecção de Dados
Rua de S. Bento, 148, 3º
1200-821 Lisboa
PORTUGAL
Tel: (+351) 213 928 400
Fax: (+351) 213 976 832
www.cnpd.pt

In the context of disclosure of information, account is taken of the possible existence of information which could pose a threat to crime prevention and criminal investigations or State security as applicable.

Disclosure is carried out by the National Data Protection Agency.

4. References to the main national laws that apply

The law applicable is Law No 67/98 of 26 October 1998 (Article 11(2)) and Law No 2/94 of 19 February 1994.

XXIII. SLOVAK REPUBLIC

1. Nature of right of access

Under Article 109 of the Convention anyone has the right to have access to data entered in the Schengen Information System (SIS) which relate to him. This right is to be exercised in accordance with national law of the contracting party. In the case of the Slovak Republic, the data subject has a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access should be addressed to the Ministry of Interior, which is the data controller:

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Pribinova 2, 812 72 Bratislava
Slovenská republika
Phone: 02/5094 1111
Fax: 02/5094 4397
send the mail
Internet :http://www.minv.sk

3. Formalities for the request: information and documents to be supplied

Under Article 69c of Act No. 171/1993 Coll. on the Police Force everyone has right to request, in writing, that the Ministry of Interior provide information on what personal data is being processed on them. At the same time the controller of the Schengen Information System is obliged to provide the information free of charge within 30 days from the date of receiving such **written request.**
The standard application form for the above request is available on the web site of the Ministry of Interior. The data subject is obliged to provide his/ her personal data (name, surname, permanent address, place and full date of birth and nationality) as well as a copy of his/her ID card or passport for the purpose of proving his/her identity.

4. Expected outcome of requests for access. Content of the information supplied

Provision of personal data to the applicant from the information systems operated by police is executed under Article 69c of the Act No. 171/1993 Coll. on the Police Force.
In the case of the Schengen Information System, if the alert was issued under Articles 95 - 98 and Article 100 of the Schengen Convention, the applicant will be informed of the data relating to him/ her (at least the following personal data: name, surname, date and place of birth, sex, nationality and reason for the alert i.e. the purpose of the processing of his/her personal data).

Where the right of access to information concerns an alert which was not issued by the Slovak Republic, the issuing county must be given an opportunity to state its position as to the possibility of disclosing the data to the applicant.
If the alert was issued under Article 99 of the Schengen Convention, the applicant is likely to be refused disclosure of the data (the processing has been carried out on national security grounds or in the investigation of particularly serious offences).

In other words, communication of information to the data subject is to be refused if essential for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties. In any event, it must be refused throughout the period of validity of an alert for the purpose of discreet surveillance.

Under Art. 69c of Act No. 171/1993 Coll. on the Police Force the data subject also has a right to **apply in writing** to the Ministry of Interior for correction or deletion of his/ her personal data processed in the Schengen Information System (a standard form concerning the request for deletion/correction of data is available on web site of the Ministry of the Interior).

If the data subject suspects that his/her personal data are being processed without authorization, under Article 20 par. 6 of the Data Protection Act he/she may lodge a **complaint** directly with the Office for Personal Data Protection of the Slovak Republic, who consequently check if there is any violation of data subject rights in the course of processing and use of personal data on the data subject held in the Schengen Information System.

Bringing complaints is regulated by the provisions of Art 45 of Act. No. 428/2002 Coll. on Protection of Personal Data (the standard form for lodging complaints is available on the web site of the Ministry of the Interior too).

5. Contact details of the national data protection agency and its possible role

Úrad na ochranu osobných údajov Slovenskej republiky
Odborárske nám. 3
817 60 Bratislava 15
Slovenská republika
Tel:+421 2 502 39 418
Fax: +421 2 502 39 441
e-mail:statny.dozor@pdp.gov.sk
Internet:http:// www.dataprotection.gov.sk

6. References of the main national laws that apply

Act No. 428/2002 Coll. on Protection of Personal Data, as amended by later legislation.

XXIV. SLOVENIA

1. Nature of right of access

There is a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Applications can be filed in written form or also orally, for the record, with the Police (Ministry of the Interior). The address is the following:

Policija, Ministrstvo za notranje zadeve
Štefanova 2
1501 Ljubljana
Slovenia
Fax: + 386 1 428 47 33
E-mail: gp.mnz(at)gov.si

Applications may also be filed at all border crossing points, administrative units and Slovenian diplomatic and consular authorities abroad. They are submitted to the Police immediately.

Link to the form for Request for Information on Data in the National Schengen Information System in Slovenia (N.SIS), which can be downloaded in English:
http://www.ip-rs.si/index.php?id=346

3. Formalities for the request: information and documents to be supplied – possible costs

The process of exercising the right to consult one's own personal data in Slovenia is regulated in accordance with the Personal data protection act (Articles 30 and 31) and the Information commissioner act.

Article 30 of the Personal data protection act requires the Police, which is subordinate to the Ministry of the Interior and a data controller, to:

1. enable consultation of the SIS filing system catalogue;

2. certify whether data relating to the data subject are being processed or not, and enable him to consult personal data contained in the national SIS filing system that relate to him, and to transcribe or copy them;

3. supply him with an extract of personal data contained in the national SIS filing system that relate to him;
4. provide a list of data recipients to whom personal data were supplied, stating when, on what basis and for what purpose;
5. provide information on the sources on which records about the individual in the SIS are based, and on the method of processing;
6. provide information on the purpose of processing and the type of personal data being processed in the SIS, and all necessary explanations in this connection;
7. explain the technical and logical-technical procedures of decision-making.

The processing of applications is at present free of charge. The requesting individual may be charged only material costs for photocopying as stipulated in the Rules on the charging of costs related to the exercise of the right of an individual to access his own personal data.

4. Contact details of the national data protection agency and its possible role

Informacijski pooblaščenec
(Information Commissioner)
Vošnjakova 1
p.p. 78
1001 Ljubljana
Slovenia
Tel.: ++ 386 1 230 97 30
Fax: ++ 386 1 230 97 78
E-mail: gp.ip@ip-rs.si
Internet: www.ip-rs.si

The Information Commissioner is competent for deciding on an appeal by an individual when a request to consult his personal data has been refused or the competent authority has refused to answer his application.

Applicants who consider that any of their rights have been violated in relation to an application for access may lodge a claim with the Information Commissioner. The Information Commissioner, having received the complaint, forwards it to the controller of the file, so that he can draw up any statements he regards as relevant. Finally, the Information Commissioner takes a decision on the complaint and forwards it to those concerned, after receiving the statements and the reports, evidence and other investigation documents, as well as inspection of the files where necessary and interviews with the person concerned and the controller of the file.

The processing of this appeal is at present free of charge.

5. Expected outcome of requests for access. Content of the information supplied

If the data relating to the person concerned are contained in the SIS file and if the request is granted, the controller of the file will provide the person concerned with the data relating to him in the form requested. The Police must enable the individual to consult, transcribe, copy and obtain a certificate no later than 15 days from the date of receipt of the request, or within the same interval, inform the individual in writing of the reasons for refusal. The Police is obliged to supply the extract mentioned above in point 3, the list in point 4, the information in points 5 and 6 and the explanation in point 7 to the individual within 30 days from the date the request was received, or, within the same interval, to inform him in writing of the reasons for refusal.

Likewise, the individual's right to consult personal data that relate to him may also be exceptionally restricted in accordance with the Article 36 of the Personal Data Protection Act, by statute, for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others. These restrictions may only be imposed to the extent necessary to achieve the purpose for which the restriction was provided.

6. References of the main national laws that apply

- Personal Data Protection Act (Official Gazette of the Republic of Slovenia, no. 94/2007, official consolidated text), unofficial English translation of the Act available at: http://www.ip-rs.si/index.php?id=339;
- Information Commissioner Act (Official Gazette of the Republic of Slovenia, no. 113/2005), unofficial English translation of the Act available at: http://www.ip-rs.si/index.php?id=325;
- Rules on the charging of costs related to the exercise of the right of the individual to access own personal data (Official Gazette of the Republic of Slovenia, no. 85/2007), only Slovene text of the Rules available at: http://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnih-podatkov/pravilnik-o-zaracunavanju-stroskov-pri-izvrsevanju-pravice-posameznika-do-seznanitve-z-lastnimi-osebnimi-podatki/.

XXV. SPAIN

1. Nature of right of access

Data subjects have a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access to information should be submitted to:

Secretaría de Estado de Seguridad
Ministerio del Interior
Amador de los Ríos, 2
E – 28010 Madrid
Tel.: 060
Fax: ---
Email: estafeta@mir.es
Internet: www.mir.es

3. Formalities for the request: information and documents to be supplied – possible costs

Any request for access must be submitted in writing to the data controller (Secretaria de Estado de Seguridad del Ministerio del Interior). To this end, data subjects must send an application to the data controller by any means that provides evidence of the dispatch and receipt of the application.

There is no a standard application form or any formal requirements. Nevertheless, following the general administrative procedure, the application should provide a full description of the request and must be accompanied by a photocopy of a document proving the identity of the data subject – i.e. a national identity card or passport. In addition, data subjects can attach to the request copies of any relevant documents they consider important in support of the request described in the application.

The procedure is free of charge.

4. Contact details of the national data protection agency and its possible role

Agencia Española de Protección de Datos (Data Protection Authority)

C/ Jorge Juan, 6
E - 28001 – Madrid
Tel.: + 34 901 100 099
Fax: + 34 91 445 56 99
E-mail: ciudadano@agpd.es
Internet: www.agpd.es

As already mentioned, data subjects have the right of direct access. Nevertheless, they also have

indirect access through the Spanish Data Protection Authority (hereinafter referred to as the Spanish DPA) when a data controller fails to respond to a request for access made by a data subject or when the answer provided is unsatisfactory. In both cases, data subjects can lodge a claim with the Spanish Data Protection Authority. Under section 117 of Royal Decree 1720/2007, that approves the regulation implementing the Organic Act 15/1999, on the Protection of Personal Data, the procedure is to be initiated at the request of the data subject, clearly expressing the content of his/her claim and the provisions of the aforementioned Spanish Data Protection Act that he/she considers breached.

Once the Spanish Data Protection Authority has received the claim, a procedure to protect rights of individuals is initiated. According to this procedure, the Spanish DPA forwards the claim to the data controller in order to give the administrative body the opportunity to lodge any defence it deems appropriate to support the denial of access or the answer provided to the applicant.

These comments, if any, are forwarded to the applicant, who can make further statements and comments. These comments are forwarded to the data controller, which has the opportunity to provide explanations of its decision and respond to the comments and statements made by the applicant.

Having received the statement of defence and the other statements and documents, the Director of the Spanish DPA delivers a decision resolving the claim received.

It is important to stress that the time-limit for issuing and notifying the decision is six months following the date of receipt of the claim at the Spanish Data Protection Authority.

If the decision is in favour of the request, the Spanish DPA communicates it to the data controller, who must grant the data subject exercise of the right of access within ten days following the notification. Moreover, the data controller is obliged to provide written evidence of compliance with the decision of the Spanish Data Protection Agency to this supervisory authority within the same period of time.

5. Expected outcome of requests for access. Content of the information supplied

If the alert was issued by the Spanish authorities, it is for the controller to decide on the content of the information supplied to applicants. Usually, the data subject receives copies of administrative documents containing personal data stored in the filing system.

However, if the alert was issued by the authorities of another Schengen country, the controller must inform its counterpart in that country of the claim received, in accordance with the principle of cooperation between national authorities with regard to the protection of personal data. It is for the authorities of the other Schengen country to decide what information can be supplied to the data subject.

6. Language regime

A data subject who wants to start the procedure for the right of access in Spain should address the public bodies in Spanish.

XXVI. SWEDEN

1. Nature of right of access

There is a right of direct access.

2. Contact details of the body to which requests for access should be addressed

Requests for access must be made to the National Police Board (Rikspolisstyrelsen), which is the authority responsible for the Swedish unit of the Schengen Information System.

Rikspolisstyrelsen
Box 12256
Polhemsgatan 30
S - 102 26 Stockholm
Tel.: ++46 (0)8-401 90 00
Fax: ++46 (0)8-401 99 90
E-mail: rikspolisstyrelsen@polisen.se
Internet: www.polisen.se

3. Formalities for the request: information and documents to be supplied – possible costs

Requests must be made in writing to the National Police Board and signed personally by the applicant. In general, a request for access must be answered within one month. Applicants are entitled to free access to information once every calendar year.

4. Contact details of the national data protection agency and its possible role

Datainspektionen
Box 8114
Fleminggatan 14, 9th floor
S - 104 20 Stockholm
Tel.: ++46 (0)8-657 61 00
Fax: ++46 (0)8-652 86 52
E-mail.: datainspektionen@datainspektionen.se
Internet: www.datainspektionen.se

The Data Inspection Board makes sure that personal data processing in Sweden complies with the rules in the Personal Data Act and other data protection legislation. The Board may initiate supervision either based on a complaint or on its own initiative. A person who is not satisfied with how his/her request for access to information in the SIS has been dealt with may submit a complaint to the Data Inspection Board. The complaint may result in an investigation of whether the rules on right of access have been complied with. The National Police Board's decision regarding the right of access may however also be appealed to administrative court.

5. Expected outcome of requests for access. Content of the information supplied

Whether or not the information is disclosed depends on the provisions of the Secrecy Act (1980:100), which may prohibit the disclosure of certain data. Where disclosure of the data is permitted, the National Police Board is responsible for forwarding it.

6. References to the main national laws that apply

Law applicable: Sections 26 and 27 of the Personal Data Act (1998:204), and Section 8 of the Schengen Information System Act (2000:344).

7. Language regime

There are no specific rules concerning this subject in Sweden. An application in English would be accepted.

XXVII. SWITZERLAND

1. Nature of right of access

There is a right of direct access. The competent authority processing individuals' requests regarding the right of access to personal data in the SIS is the Data Protection Officer of the Federal Office of Police in Switzerland.

2. Contact details of the body to which requests for access should be addressed

Federal Office of Police
Data Protection Officer or SIRENE Office
Nussbaumstrasse 29
CH-3003 Berne
www.fedpol.ch

3. Formalities for the request: information and documents to be supplied – possible costs

Individuals' requests concerning their personal data processed in the SIS have to be directly addressed to the Federal Office of Police, controller of the SIS data file in Switzerland (only written requests, with a copy of a valid identity card or passport).

4. Contact details of the national data protection agency and its possible role

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1,
CH-3003 Berne
Phone: +41(0)31 322 43 95, Fax +41-(0)31 325 99 96
www.edoeb.admin.ch

Only verification requests are to be addressed to the Federal Data Protection and Information Commissioner (FDPIC) in Switzerland, the federal level of the national data protection authority.

ANNEXES (MODEL LETTERS)

Annex 1

Model letter for requesting access

To: **Title and address of the competent authority**

DD-MM-XXXX,

Place

Dear Sir / Madam,

Pursuant to Article 109 of the Schengen Convention,

I_____(name, surname),_____(nationality),

_____(date and place of birth),_____(address), would like to request access to my personal data entered in the Schengen Information System.

Please find enclosed:

1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document);
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant / The Legal Representative

(Signature)

Annex 2

Model letter requesting a check

To: **Title and address of the competent authority**

DD-MM-XXXX,
Place

Dear Sir / Madam,

Pursuant to Article 114(2) of the Schengen Convention,
I_____(name, surname),_____(nationality),
_____(date and place of birth),_____(address), would like to request a check on my personal data entered in the Schengen Information System and the use made of my data.

Please find enclosed:
1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document);
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant/The Legal Representative

(Signature)

Annex 3

Model letter for correction

To: **Title and address of the competent authority**

DD-MM-XXXX,

Place

Dear Sir / Madam,

Pursuant to Article 110 of the Schengen Convention,

I_____(name, surname),_____(nationality),

_____(date and place of birth), _____(address),

would like to request correction of factually inaccurate data relating to me or deletion of data relating to me which have been unlawfully stored in the Schengen Information System. My personal data should be corrected/deleted because:

_____

_____

_____

_____

Please find enclosed:

1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document);
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant/The Legal Representative

(Signature)