THE SCHENGEN INFORMATION SYSTEM

A GUIDE FOR EXERCISING DATA SUBJECTS' RIGHTS:

THE RIGHT OF ACCESS, RECTIFICATION AND ERASURE

Secretariat postal address: Rue Wiertz 60, B-1047 Brussels
Offices: Rue Montoyer 30, B-1000 Brussels
E-mail : csc-secretariat@edpb.europa.eu

This guide was compiled by the SIS II Supervision Coordination Group.

The national contributions, and any translations of this guide into languages other than English, are the responsibility of each national supervisory authority and they do not necessarily reflect the official position of the CSC. The CSC does not guarantee the accuracy of the information included in the national contributions and any questions should be address to the respective national supervisory authorities. Neither the CSC nor any person acting on the CSC's behalf may be held responsible for the use which may be made of the information contained therein.

Secretariat postal address: Rue Wiertz 60, B-1047 Brussels
Offices: Rue Montoyer 30, B-1000 Brussels

E-mail : csc-secretariat@edpb.europa.eu

TABLE OF CONTENTS

1. Introduction to the Schengen Information System (SIS) 5
   1.1. Legal basis 6
   1.2. Categories of information processed (alerts) 7
   1.3. Categories of personal data processed 8
2. Rights recognised to individuals whose data is processed in the SIS 9
   2.1. Right of access 10
   2.2. Rights to rectification and erasure of data 11
   2.3. Remedies: the right to complain to the data protection authority or to initiate a judicial proceeding 12
3. Description of the procedure for the exercise of the rights in each Schengen State 12
3.1. AUSTRIA 13
3.2. BELGIUM 14
3.3. BULGARIA 17
3.4. CROATIA 20
3.5. CZECH REPUBLIC 22
3.6. DENMARK 24
3.7. ESTONIA 26
3.8. FINLAND 28
3.9. FRANCE 30
3.10. GERMANY 33
3.11. GREECE 35
3.12. HUNGARY 38
3.13. ICELAND 40
3.14. IRELAND 42
3.15. ITALY 45
3.16. LATVIA 47
3.17. LUXEMBOURG 50
3.18. LIECHTENSTEIN 53
3.19. LITHUANIA 55

3.20. MALTA 57
3.21. NETHERLANDS 60
3.22. NORWAY 63
3.23. POLAND 66
3.24. PORTUGAL 73
3.25. ROMANIA 75
3.26. SLOVAK REPUBLIC 78
3.27. SLOVENIA 81
3.28. SPAIN 84
3.29. SWEDEN 88
3.30. SWITZERLAND 90
Annex 1 92
Model letter for requesting access 92
Annex 2 92
Model letter for requesting rectification 93
Annex 3 94
Model letter for requesting erasure 94

Any individual is guaranteed the right of access to his/her own data, the right to rectification of inaccurate data and the right to erasure of unlawfully stored data in the Schengen Information System (hereinafter 'SIS')[1].

This Guide describes the modalities for exercising those rights. This is the most updated version, of 21 November 2022, to reflect the changes brought by the current SIS legal framework and the revision of the EU data protection framework, since the SIS Regulations are now referring to the exercise of some rights as laid down in the GDPR[2] and in the Law Enforcement Directive[3].[4]

The Guide is divided into three sections: (1) a description of the SIS, of (2) the rights granted to the individuals whose data are processed in SIS and (3) a description of the procedure for exercising the rights in each of the countries concerned.

As annex to the Guide, it is also made available three model letters to be used by applicants to file the requests of access, rectification and erasure, unless the national competent authority to which the request is addressed requires the use of a specific standard form.

1. INTRODUCTION TO THE SCHENGEN INFORMATION SYSTEM (SIS)

The SIS is a large-scale IT system, set up as a compensatory measure for the abolition of internal border checks, and intends to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States. The SIS is already implemented in all EU Member States, with the exception of Cyprus[5], and in four Associated States: Iceland,

[1] These rights are granted under Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1
[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.
[4] Cfr. Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862.
[5] Information dated from October 2022. Croatia is connected to the SIS with some limitations that are expected to be overcome in 2024. Ireland operates SIS for law enforcement purposes only.

Liechtenstein, Norway and Switzerland.

The SIS is an information system that allows national law enforcement, judicial and administrative authorities to perform their legal tasks by sharing relevant data. With regard to the European agencies, they have read-only access; i.e. the possibility to search and consult the SIS but not to update or delete the data or the alerts. EUROPOL has access to all categories of alerts stored in SIS[6], while EUROJUST[7] has access to specific alerts in the field of police and judicial cooperation, and the European Border and Coast Guard (EBCG)[8] has limited access to the SIS for certain teams and for specific purposes.

1.1. Legal basis

In 2018, the SIS legal framework went through a significant revision primarily to enlarge its purposes, to add certain categories of alerts, and to expand the authorities with granted access to SIS data. The new legal framework was adopted on 28 November 2018 and published on 7 December 2018[9].
It consists of three new Regulations, covering three areas of competence:

- Regulation (EU) 2018/1860[10] ("SIS Regulation on the use of SIS for the return of illegally staying third-country nationals")[11],
- Regulation (EU) 2018/1861[12] ("SIS Regulation in the field of border checks")[13],

[6] Article 35(1) of Regulation (EU) 2018/1861 and Article 48 (1) of Regulation (EU) 2018/1862.
[7] Article 49 (1) of Regulation (EU) 2018/1862.
[8] Article 36 (1) of Regulation (EU) 2018/1861 and Article 50 (1) of Regulation (EU) 2018/1862.
[9] Initially, they were supposed to become fully applicable by 28 December 2021(Article 20 of Regulation 2018/1860, Article 66 (2) Regulation 2018/1861 and Article 79 of Regulation 2018/1862); however due to delays in the implementation of the new functionalities of the system, the new Regulations only became fully applicable since 7 March 2023.
[10] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312, 7.12.2018, p. 1.
[11] The SIS Regulation for return is applicable to all Member States and associated Schengen States, with the exception of Ireland.
[12] Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018, p. 14.
[13] The SIS Regulation in the field of border checks applies to all Schengen States.

- Regulation (EU) 2018/1862[14] ("SIS Regulation in the field of police and judicial cooperation"), as amended by Regulation (EU) 2022/1190[15]

The SIS will become, in the near future, interoperable with five other EU-large information systems[16], pursuant to the full application of the Interoperability Regulations[17]. This fact, among other things, will have an impact on the exercise of data subjects' rights in this context. By then, this Guide will be updated accordingly.

1.2. Categories of information processed (alerts)

The SIS contains two broad categories of information: alerts on *persons* and alerts on *objects*. With regard to alerts on persons, SIS covers the following categories of data subjects:

- third country nationals subject to refusal of entry or stay in the Schengen area or subject to return procedures,
- persons wanted for arrest for surrender or extradition purposes (in the case of associated countries),
- missing persons (including vulnerable persons who need to be prevented from travelling, e.g., children at high risk of parental abduction, children at risk of becoming victims of trafficking in human beings, and children at risk of being recruited as foreign terrorist fighters),
- persons sought to assist with a criminal judicial procedure,
- persons subject to discreet, inquiry or specific checks,
- unknown wanted persons who are connected to a crime (e.g. persons whose fingerprints are found on a weapon used in a crime),

[14] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56.

[15] Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, OJ L 185, 12.7.2022, p. 1.

[16] VIS, Eurodac, EES, ETIAS and ECRIS-TCN.

[17] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, p. 27;
Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85.

- Information on third country nationals in the interest of the Union ("information alerts").

These last two alerts are brand new in the SIS, introduced by the SIS Recast. While other alerts have been considerably modified by the new legal framework, such as the alert on missing persons or the alert on discreet or specific checks.

With regard to the alerts on objects, SIS stores data on objects sought for the purpose of seizure or use as evidence in criminal proceedings, or subject to discreet or specific checks. Such objects include vehicles, boats, firearms, identity documents stolen, misappropriated, lost or invalidated, bank notes, credit cards, blank documents, and as a new category "objects of high value" (e.g., items of information technology, which can be identified and searched with a unique identification number).

1.3. Categories of personal data processed

When the alert concerns a person (with the exception of unknown wanted person), the information must always include: the surname, date of birth, the reason for the alert, the gender, a reference to the decision giving rise to the alert, the basis for the decision for refusal of entry and stay (when applicable), the action to be taken, last date of the period for voluntary departure if applicable, whether return is accompanied by an entry ban. If available, the alert may also contain information such as, any specific, objective, physical characteristics not subject to change; the place of birth; photographs; fingerprints; nationality(ies); whether the person concerned is armed, violent or has escaped; the authority issuing the alert; links to other alerts issued in SIS in accordance with Article 48 of Regulation (EU) 2018/1861 or Article 63 of Regulation (EU) 2018/1862.

When the alert concerns unknown wanted persons, only dactyloscopic data may be processed, either complete or incomplete sets of fingerprints or palm prints, which due to their unique character and the reference points contained therein should enable accurate and conclusive comparisons on a person's identity[18].

[18] According to the definition provided by Article 3 (13) of Regulation (EU) 2018/1862.

2. RIGHTS RECOGNISED TO INDIVIDUALS WHOSE DATA IS PROCESSED IN THE SIS

Data subjects shall be able to exercise the rights in relation to their personal data processed in the SIS, as laid down in Articles 15, 16 and 17 of the GDPR and in Articles 14 and 16 (1) and (2) of the LED, and in accordance with the SIS Regulations[19]. In addition, data subjects are entitled to seek remedies to enforce such rights[20].

Therefore, data subjects have the following rights:

- right of access to data relating to them processed in the SIS;
- right to rectification of inaccurate data;
- right to erasure when data have been unlawfully stored;
- right to bring an action before the courts or competent supervisory authorities to access, rectify, erase, obtain information or obtain compensation in connection to an alert concerning them.

Anyone exercising any of these rights can apply to the competent authorities in a Schengen State of his or her choice. This option is possible because all national databases (N.SIS) are identical to the central system database (CS.SIS)[21]. Consequently, these rights can be exercised in any Schengen country regardless of the State that issued the alert.

However, the Member State receiving the request from the data subject has to consult previously the Member State issuing the alert before providing any information to the data subject about the data processed in the SIS.

To assist data subjects in exercising their rights, this Guide publishes in its Part 3 the list of national authorities competent to handle data subjects' requests, how these are to be addressed, including any national requirements, and what means are made available for that purpose.

Regardless of specific national procedures to handle the application for access, rectification or erasure of data processed in the SIS, the reply to the data subject is due within a strict common

[19] See 53 of Regulation (EU) 2018/1861 and 67 of Regulation (EU) 2018/1862.
[20] See Article 54 of Regulation (EU) 2018/1861 and Article 68 of Regulation (EU) 2018/1862.
[21] See Article 4(1)(b) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862.

deadline. The data subject shall be informed as soon as possible, and, in any event, within one month of receipt of the request, about the follow-up given to the exercise of the right. This period may be extended by two further months where necessary and in such case, the data subject shall be informed of any such extension within one month of receipt of the request, together with the reasons for the delay[22].

2.1. Right of access

The right of access is the possibility for anyone who so requests to have knowledge of whether or not information relating to him or her are processed by a public or private organisation, and to receive information on these data. This is a fundamental right, enshrined in Article 8 (2) of the EU Charter of Fundamental Rights, and its exercise is instrumental to put into effect other data protection rights and to protect in general the freedoms and rights of individuals.

The right of access in what concerns the data processed in the SIS is provided for in Article 53(1) of Regulation (EU) 2018/1861 and in Article 67(1) of Regulation (EU) 2018/1862[23], which refer to the right of access laid down in Article 15 of the GDPR and Article 14 of the LED.

This means that data subjects have the right to obtain confirmation as to whether or not personal data concerning them are being processed in the SIS and, where that is the case, access to the personal data and the following information:

- The purpose of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been disclosed, in particular in third countries or international organisations;
- The envisaged period for which the personal data will be stored;
- The existence of the right to request rectification of inaccurate data or erasure of unlawfully stored data;
- The right to lodge a complaint

[22] See Article 53(4) of Regulation (EU) 2018/1861 and 67(4) of Regulation (EU) 2018/1862, which refers to the deadlines provided in Article 12(3) of the GDPR.

[23] Both Articles state : 'Data subjects shall be able to exercise the rights laid down in Articles 15 (…)of Regulation (EU) 2016/679 and in Article 14 (…)of Directive (EU) 2016/680.[…]'

- Communication of the source of the information when data is collected from a third party.

However, the right of access is exercised in accordance with the law of the Member State where the request is submitted, and there could be restrictions to access the data, i.e. a decision not to provide information, wholly or in part, to the data subject. This is possible to the extent that such limitation constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:

- avoid obstructing official or legal inquiries, investigations or procedures;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others[24].

Where that is the case, the applicant shall be informed in writing, without undue delay, of any refusal or restriction, unless the provision of such justification undermines one of the above-mentioned objectives. The authority receiving the request for access shall inform the applicant that he or she can lodge a complaint with the data protection authority or seek judicial remedy.

If there is a complete or partial refusal of access, data subjects can exercise their rights vis-à-vis the SIS through the national data protection supervisory authority. This Guide also publishes the name and contact details of the data protection supervisory authorities in each Schengen State.

2.2. Rights to rectification and erasure of data

Besides the right of access, there is also the right to obtain the rectification of personal data factually inaccurate or incomplete or the right to ask for erasure of personal data unlawfully stored (Article 53(1) of Regulation (EU) 2018/1861 and Article 67(1) of Regulation (EU) 2018/1862).

Under the Schengen legal framework, only the Member State responsible for issuing an alert in the SIS may alter or delete it (See Article 44(3) of Regulation (EU) 2018/1861 and 59(3) of Regulation (EU) 2018/1862).

[24] See Articles 53(3) of Regulation (EU) 2018/1861 and 67(3) of Regulation (EU) 2018/1862.

If the request is submitted in a Member State that did not issue the alert, the competent authorities of the Members States concerned cooperate to handle the case, by exchanging information and making the necessary verifications.

The applicant should provide the grounds for the request to rectify or erase the data and gather any relevant information supporting it.

2.3. Remedies: the right to complain to the data protection authority or to initiate a judicial proceeding

Articles 54 of Regulation (EU) 2018/1861 and 68 of Regulation (EU) 2018/1862 presents the remedies accessible to individuals when their request has not been satisfied. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, rectify, erase, obtain information or to obtain compensation in connection with an alert relating to him or her.

In case they have to deal with a complaint with a cross-border element, supervisory authorities should cooperate with each other to guarantee the rights of the data subjects.

3. DESCRIPTION OF THE PROCEDURE FOR THE EXERCISE OF THE RIGHTS IN EACH SCHENGEN STATE

The procedures specific to each country applying the Schengen acquis, which are to be followed by individuals wishing to exercise their right of access, rectification or erasure, are described in the national fact sheets in the remainder of this chapter.

3.1. AUSTRIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Bundesministerium für Inneres (BMI)
Bundeskriminalamt, SIRENE Österreich
Josef Holaubek Platz 1
1090 Vienna
AUSTRIA
E-Mail: bundeskriminalamt@bmi.gv.at

2. How to make an individual request and what to include in it?

In Austria, the right to access is direct. A request for access must be made to the Bundesministerium für Inneres (Ministry of the Interior), which is the authority responsible for the national system of the Schengen Information System.
The request has to be made in writing and must contain the signature of the applicant. The request must be accompanied by a copy of a valid and official identity document, which has to contain the name, date of birth, photograph and signature of the applicant (e.g. passport, identity card or driving licence). The Datenschutzbehörde (Austrian Data Protection Authority) provides a template (in German and English) on its website (www.dsb.gv.at). The request of access is free.
If the Ministry of the Interior does not take action on the request of the applicant within four weeks or the applicant is of the opinion that the provided information of the Ministry of the Interior is incomplete or wrong, the applicant can lodge a complaint with the Austrian Data Protection Authority.
In accordance with the Austrian constitution, the official language in Austria is German. However, the request can also be made in English.

3. Contact details of the national data protection authority

Datenschutzbehörde
Barichgasse 40-42
1030 Vienna
Austria
E-mail: dsb@dsb.gv.at
Website: www.dsb.gv.at

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

In accordance with § 44 of the Data Protection Act, every data subject shall have the right to obtain confirmation from the controller as to whether personal data concerning him or her are being processed; if this is the case, he or she shall have the right to obtain access to personal data.
In the event of a refusal to provide the information, the controller shall pursuant to § 43(4) of the Data Protection Act immediately inform the data subject in writing of the refusal or restriction of the information and the reasons for it. This shall not apply if the provision of such information would be contrary to one of the purposes mentioned in § 43(4) of the Data Protection Act, i.e. to ensure that the prevention, detection, investigation or prosecution of criminal offences or the execution of sentences are not impaired, in particular by obstructing official or judicial enquiries, investigations or proceedings, for the protection of public and national security, for the protection of the constitutional institutions of the Republic of Austria, for the protection of military self-security, or for the protection of the rights and freedoms of others. The controller shall inform the data subject of the possibility to lodge a complaint with the data protection authority.

5. References of the main national laws that apply
Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)

3.2. BELGIUM

The exercise of the rights of access, rectification and deletion concerning SIS differs according to whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.

If the request concerns an alert processed for the purposes of refusing admission or a stay in the Schengen area or return resulting from an administrative decision taken by the Belgian Immigration Office, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

In the absence of a response from the CSIS Office within the period of one month from the receipt of your request or if this answer is not satisfactory, you can lodge a complaint with the Data Protection Authority (https://www.dataprotectionauthority.be/citizen).

If your request concerns another alert introduced by the Belgian authorities (for the purposes of police and judicial cooperation in criminal matters), it must be sent to the Supervisory Body for Police Information.

Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. It means that the request must be sent to the Supervisory Body which verifies the data. According to the Belgian data protection Act (30 July 2018), the Supervisory Body only communicates to the person concerned that the necessary checks have been carried out.

1. Contact details of the body to which requests for access, correction or deletion should be addressed

For the purposes of police and judicial cooperation in criminal matters :
Supervisory Body for Police Information
Rue de Louvain 48, 1000 Brussels, Belgium
+32 (0)2 549 94 20
Info@organedecontrole.be

For the other purposes :
Immigration Office, Federal Public Service Interior
CSIS Office
Boulevard Pacheco 44, 1000 Brussels, Belgium
e-mail: csis@ibz.fgov.be

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- Data subject.
- Lawyer with power of attorney.

2.2. To whom the request should be submitted

- Concerning the purposes of police and judicial cooperation in criminal matters, the request should be sent to the Supervisory Body which verifies the data.
- Concerning the other purposes, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

2.3. How the request should be submitted

- In paper and/or electronic format, digitally signed;

- It must be written, dated and signed by the data subject or his lawyer;
- Concerning the purposes of police and judicial cooperation in criminal matters, the request can be submitted via an online form: https://www.controleorgaan.be/en/citizens/access-to-the-schengen-information-system-sis-ii ;
- Concerning the other purposes, it must be addressed via e-mail (csis@ibz.fgov.be)
- Any additional information can be provided within one month of the request.

2.4. Minimum information to be supplied

- Personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);

2.5. Documents to be supplied

- The data subject must also provide proof of identity by attaching a copy of an identity document (double-sided);
- A lawyer must provide evidence of his capacity and also attach the mandate given by his client.

2.6. Language regime

- The request can be submitted in one of the Belgian national languages or in English ;
- The reply to the applicant will be in one of the Belgian national languages or in English.

2.7. Link to website where information on how to apply for information/correction/deletion

Concerning the Supervisory Body for Police Information :
https://www.controleorgaan.be/en/citizens/access-to-the-schengen-information-system-sis-ii

Concerning the Immigration Office, Federal Public Service Interior : https://dofi.ibz.be/

3. Contact details of the national data protection authority

Concerning the purposes of police and judicial cooperation in criminal matters :
Supervisory Body for Police Information
Control and supervisory authority for the processing of data by the police, in particular in the context of the SIS
Rue de Louvain 48, 1000 Brussels, Belgium
+32 (0)2 549 94 20
Info@organedecontrole.be
www.organedecontrole.be

Concerning the other purposes :
Data Protection Authority
Rue de la Presse, 35
1000 Bruxelles
+32 (0)2 274 48 00
+32 (0)2 274 48 35
contact@apd-gba.be
www.dataprotectionauthority.be

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

4.1. Content of the notifications

The exercise of the rights of access, rectification and deletion concerning SIS differs according to

whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.

If the request concerns an alert processed for the purposes of refusing admission or a stay in the Schengen area or return resulting from an administrative decision taken by the Belgian Immigration Office, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

If your request concerns another alert introduced by the Belgian authorities (for the purposes of police and judicial cooperation in criminal matters), it must be sent to the Supervisory Body for Police Information.

Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. This signifies that the request must be sent to the Supervisory Body which will verify the data. According to the Belgian data protection Act (30 July 2018), the Supervisory Body only communicates to the person concerned that "*the necessary checks have been carried out*". The Supervisory Body can therefore never provide you with any concrete information concerning the processed data.

4.2. Procedure to submit a complaint

Concerning the purposes of police and judicial cooperation in criminal matters, the Belgian data protection Act provides for a procedure in Article 209.
This action must be brought against the controller.

Concerning the other purposes, in the absence of a response from the CSIS Office within the period of one month from the receipt of your request or if this answer is not satisfactory, a complaint can be lodged with the Data Protection Authority (https://www.dataprotectionauthority.be/citizen).

5. References of the main national laws that apply

5.1 Act on the protection of natural persons with regard to the processing of personal data, 30 July 2018

5.2 Specific elements

The exercise of the rights of access, rectification and deletion concerning SIS II differs according to whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.
Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. It means that the request should be sent to the Supervisory Body which verifies the data. According to the Belgian data protection Act, the Supervisory Body only communicates to the person concerned that the necessary checks have been carried out.
Concerning the other purposes, this a direct procedure with the Immigration Office, Federal Public Service Interior, CSIS Office.

3.3. BULGARIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministry of Interior of the Republic of Bulgaria
SIRENE Bureau at the Ministry of Interior (International Operational Cooperation Directorate)
Address:1146 Knyaginya Maria Luiza Blvd, Sofia 1233, Bulgaria
Tel.: +359 2 9825 000
Fax: +359 2 9153 525
Email: priemna@mvr.bg
Web site: https://www.mvr.bg/

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every individual has the right of access to his/her personal data, processed in Ministry of Interior's (MoI) information funds or SIS.
The individual should submit access request directly to the national SIRENE Bureau, established as a unit in the International Operative Cooperation Directorate of the MoI.
Such request could be submitted to the Commission for Personal Data Protection (CPDP) as well, which will forward it to the MoI.

2.2. How the request should be submitted

The request can be submitted in person, on paper (via post) and/or in electronic format signed with qualified electronic signature by the data subject, by lawyer with power of attorney or legal guardian, if necessary. The data subjects can be represented by appointed lawyer or legal guardian.

On CPDP's official site are provided model letters for requesting information from SIS II, as follows:
https://www.cpdp.bg/en/index.php?p=element&aid=1310 – In English

The Minister of Interior is obliged to take a decision within 14 days from the receipt of the access request.
A copy of the individual's processed personal data can be provided on paper upon request.
The submission of request for access to SIS data is free of charge.

2.3. Minimum information to be supplied

The minimum supplied applicant personal data is:name, surname, date of birth, nationality, gender, citizenship and information about passport validity.
Model forms for exercising the rights of access, correction or deletion of data can be found on the CPDP's official site:
https://www.cpdp.bg/en/index.php?p=element&aid=1310 – in English

In the model letters as reasons for the correction/deletion of personal data are set inaccuracy or unlawful storage.

2.4. Documents to be supplied

The documents that need to be supplied for the request are:

- proof of applicant's identity- readable copy of ID or passport
- proof of granted power of attorney- when necessary
- notarial verified letter of attorney (in case of authorisation of representation by third party)

2.5 Language regime

The languages that can be used when submitting the request are Bulgarian and English.
The language used to reply to the applicant if he/she isn't Bulgarian citizen is English.

2.6. Link to website where information on how to apply for information/correction/deletion

The link to apply for information/correction/deletion of personal data in SIS II is:
https://www.cpdp.bg/en/index.php?p=element&aid=1310 – in English

3. Contact details of the national data protection authority

Commission for Personal Data Protection
Sofia 1592, 2 "Prof. Tsvetan Lazarov" blvd.
Tel.: + 3592/91-53-519
Fax: +3592/91-53-525
E-mail: kzld@cpdp.bg
Web site: www.cpdp.bg.

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

4.1. Content of the notifications

In accordance with Art. 15 (1) and (2) of the in Ordinance No. 8121з-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria (Prom. SG 74/5 September 2014, last amend. and suppl. SG 23/22 March 2022), the data subject has right to access, correct or request deletion of his/her inaccurate or unlawfully processed personal data in N.SIS.

The data subjects' rights are exercised under the conditions and following the procedures set in the Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862, Ministry of Interior Act and the Personal Data Protection Act.

4.2. Procedure to submit a complaint

Complaints about violations of the individual's rights for access, correction or deletion of his/her personal data in SIS II can be submitted following the requirements described on the CPDP's official site:
https://www.cpdp.bg/en/index.php?p=pages&aid=56 - in English

5. References of the main national laws that apply

- Ministry of Interior Act (MIA) (Prom. SG 52/27 June 2014, last amend. and suppl. SG 62/5 August 2022) and the related secondary legislation - e.g. the specific rules for the organization and operation of the national system (N.SIS) are set out in Ordinance No. 8121з-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria (Prom. SG 74/5 September 2014, last amend. and suppl. SG 23/22 March 2022). In accordance with Article 14 of the Ordinance, data processing at N.SIS is carried out in compliance with the Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862, Ministry of Interior Act and the Personal Data Protection Act and the subsidiary legislation, related to their application.

Certain aspects of personal data protection, related to SIS II, are also regulated by other legal acts, such as:

- the Administrative Procedure Code (Prom. SG 30/11 April 2006, last amend. and suppl. SG 15/19 February 2021)- judicial control;
- the Penal Code (Prom. SG 26/2 April 1968, last amend. and suppl. SG 53/8 July 2022);
- the Penal Procedure Code (Prom. SG 83/18 October 2005, last suppl. SG 62/5 August 2022);
- the Foreigners in the Republic of Bulgaria Act (Prom. SG 153/23 December 1998, last amend. SG 22/18 March 2022);
- the Extradition and European Arrest Warrant (EAW) Act (Prom. SG 46/3 January 2005, last amend. and suppl. SG 45/7 June 2019);
- the Bulgarian Personal Documents Act (Prom. SG 93/11 August 1998, last amend. SG 32/26 April 2022);
- the Customs Act (Prom. SG 15/6 February 1998, last suppl. SG 62/5 August 2022);
- the State Agency for National Security Act (Prom. SG 109/20 December 2007, suppl. SG 51/5 June 2020);
- the Act on entering, residing and leaving the Republic of Bulgaria by European Union citizens and their family members (Prom. SG 80/3 October 2006, amend. and suppl. SG 21/12 March 2021);
- Asylum and Refugees Act (Prom. SG 54/31 May 2002, last amend. SG 32/26 April 2022);
- the Administrative Violations and Penalties Act (Prom. SG. 92/28 November 1969, last suppl. SG 51/1 July 2022- judicial control.

The requests for access/correction/deletion of personal data in N.SIS can be send in Bulgarian and English.

The alerts storage deadlines can be prolonged in case it is necessary for the achievement of their purposes. The prolongation necessity is revised by the authority, which has entered the alert one month after the set deadlines have expired (for alerts on persons) and after the expiration of the half storage term and two months before the deadline expiration (for alerts on objects- discreet checks and for or seizure or use as evidence in criminal proceedings).

With regard to third country citizens alerts with imposed restrictions for entering and stay (alerts for persons for arrest, for surrender or extradition purposes) the necessity for prolongation is revised within three/five years from their entering depending on the imposed restrictions deadlines.

The SIS alerts for persons and objects are automatically deleted after the set storage deadline under the conditions set in Art.55 of Regulation (EU) 2018/1862, if the further retention is not necessary.

The alerts for third country citizens, who are with revoked right to stay in Bulgaria or are due to be returned to their country or expulsed are deleted under the conditions set in Art.6 (2), Art. 8, it.”b”, Art. 9 (2), Art. 11, it. “f” and Art. 14 of Regulation (EU) 2018/1860.

The alerts for third country citizens, who are prohibited to enter and reside on the territory of Member States of the European Union or are subject to issued orders for imposture of compulsory administrative measures are deleted under the conditions set in Art. 40 of Regulation (EU) 2018/1861.

In cases of identity theft and the additional processing of the victim personal data, these data are deleted simultaneously with the relevant alert or earlier upon victim’s request.

3.4. CROATIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Contact details of Ministry of the Interior, the body to which request for access, correction or deletion should be addressed is:

Ministarstvo unutarnjih poslova
Ulica grada Vukovara 33
HR - 10 000 Zagreb

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Only natural person – data subject can submit a request. It is not envisaged that request can be submitted by layer with power of attorney or legal guardian.

2.2. How the request should be submitted
Request must be submitted in written form to the data controller using templates available on its web site:

- Access https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20pristup%20osobnim%20podacima%20koji%20su%20obra%C4%91eni%20u%20SISII.pdf
- Correction: https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20ispravak%20osobnih%20podataka%20koji%20su%20obra%C4%91eni%20u%20SISII.pdf
- Deletion: https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20brisanje%20osobnih%20podataka%20koji%20su%20obra%C4%91eni%20u%20SISII.pdf

Data subjects must send an application personally signed to the data controller using regular post service. It is not envisaged that request can be submitted by e-mail.
If data subject submit request for access, correction or deletion to national Data Protection Authority, same Authority informs data subject that he/she needs to submit request to Ministry of Interior using forms available on their web site.

2.3. Minimum information to be supplied

Personal data of applicant that should be included are: name, surname, Personal Identification Number (if any), place of residence, place of birth, date of birth, nationality.

2.4. Documents to be supplied

- Documents that should be supplied as proof of identity: copy of ID or passport. Also, applicants do not need to justify their request for access/correction/deletion.

2.5 Language regime

Form is written in Croatian and English languages so it is expected that applicant can submit request on both languages. Consequently, language used for submitting request will be used for providing replay to applicant.
Structured information on how to apply for information/correction/deletion is available on both Croatian

and English versions of web site of Ministry of Interior:

- https://mup.gov.hr/zastita-osobnih-podataka/222
- https://mup.gov.hr/personal-data-protection/124

2.6. Link to website where information on how to apply for information/correction/deletion

Document specifically related with topic is further available on link: https://mup.gov.hr/UserDocsImages//dokumenti//Data-protection-and-the-Schengen-Information-System.pdf

3. Contact details of the national data protection authority

Agencija za zaštitu osobnih podataka
Selska cesta 136,
10000 Zagreb
Croatia
Tel: +385 1 4609-000
Fax: +385 1 4609-099
www.azop.hr

The Croatian Personal Data Protection Agency (hereinafter: the Agency) is the only independent public supervisory authority in the Republic of Croatia within the meaning of the provision of Article 51 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

5. References of the main national laws that apply

Croatia does not have separate national Law and it provisions that applies specifically to SIS.

The Act on the Implementation of the General Data Protection Regulation (Official Gazette, No. 44/2018) (Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne Novine 44/2018 https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html) stipulates in Art. 34. that anyone who considers that any of his or her rights guaranteed by the GDPR and the Act on the Implementation of the GDPR have been violated, may submit to the Agency a request for determination of a violation of a right. The Agency shall decide on the violation of rights by a ruling. The ruling of the Agency shall be an administrative act. No appeal shall be allowed against the ruling of the Agency, but an administrative dispute may be instituted by lodging a complaint before a competent administrative court.

If data subject considers that his rights on request for information/correction/deletion in SIS have been violated by Ministry of Interior, he/she can submit claim to the Agency.

3.5. CZECH REPUBLIC

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The Police Presidium of the Czech Republic
P. O. BOX 62/K-SOU, 170 89 Praha 7, Czech Republic
+420 974 835 775
epodatelna.policie@pcr.cz

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Requests can be submitted by a subject whose data are concerned, or by another person, who has been authorized by the subject.

2.2. How the request should be submitted

Request should be submitted in a written form (paper or digital). It is also possible to submit a request during office hours at any police station.
Link to online forms: https://www.policie.cz/docDetail.aspx?docid=22450996&doctype=ART

2.3. Minimum information to be supplied

Identification data, i.e., name and surname, date of birth, address of residence or other postal address usable for delivery shall be supplied. In case of request for data correction or deletion, the justification for the request should be provided, e.g., corrections required, description of circumstances, reasoning for deletion.

2.4. Documents to be supplied

A readable copy of any identification document should be enclosed.
If the data subject authorises another person to submit the request, a special power of attorney with a certified signature must be submitted. In cases where the data subject authorises a lawyer to submit the request, it is sufficient to provide a general power of attorney without a certified signature..

2.5 Language regime

The subject can submit his/ her request either in Czech or in English. The reply is sent to the data subjects in the Czech language.

2.6. Link to website where information on how to apply for information/correction/deletion

Information on how to apply for information, correction or deletion is available on the websites of the Police of the Czech Republic (https://www.policie.cz/docDetail.aspx?docid=22450996&doctype=ART) and the Czech national data protection authority (https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1366&p1=1366).

3. Contact details of the national data protection authority

The Office for Personal Data Protection (Úřad pro ochranu osobních údajů)
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.

Pplk. Sochora 27
170 00 Praha 7
Czech Republic
+420 234 665 111
posta@uoou.cz
www.uoou.cz

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

4.1. Content of the notifications

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

According to the § 28 (3) of the Act No 110/2019 Coll., on Personal Data Processing, 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.

4.2. Procedure to submit a complaint

If the subject does not receive a response from the controller in time or if the response is not satisfactory to the subject, he or she may contact the Office for Personal Data Protection with a complaint. Such a complaint can be submitted in person or in writing (in paper or digital form), in both Czech and English. The data subject shall prove his/her identity and provide all information supporting his/her complaint, e.g., previous communication with the data controller, including documents provided or received. Where the data subject authorises another person to submit a complaint, a special power of attorney with a certified signature must be submitted, except in the case of representation by a lawyer, where a general power of attorney will suffice.

5. References of the main national laws that apply

- Act No. 110/2019 Coll., on Personal Data Processing
- Act No 273/2008 Coll., on the Police of the Czech Republic

3.6. DENMARK

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Requests for access should be addressed to the Danish National Police:

Danish National Police
Polititorvet 14
DK-1780 København V
E-mail: pol-jur-efterforskning@politi.dk
Tel.: +45 33 14 88 88

Request for correction or deletion should be addressed to the Danish Return Agency:

The Danish Return Agency
Birkerød Kongevej 2
DK-3460 Birkerød
Tel.: + 45 30 65 78 00

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, persons or legal entities with a power of attorney, or a legal guardian can submit a request.

2.2. How the request should be submitted

There are no particular formal requirements for submitting a request. However, if at all possible, requests should be submitted electronically through the following secure contact form:

- Request-for-access
- Request for correction or deletion

2.3. Minimum information to be supplied

- Personal data of the applicant (name, surname, date of birth, nationality, contact information);
- use of model forms to exercise the rights vis-à-vis the SIS
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, residence permit, birth certificate, drivers' licence);
- proof of granted power of attorney

2.5 Language regime

Danish is the official language used for communication with the Danish authorities. However, it is also possible to communicate with the Danish authorities in English.

2.6. Link to website where information on how to apply for information/correction/deletion

For information on how to submit a request, see the websites listed below:

- Schengen Information System (SIS II) (datatilsynet.dk)
- International police cooperation | | Danish police (politi.dk)
- https://www.hjemst.dk/kontakt/

3. Contact details of the national data protection authority

Datatilsynet
Carl Jacobsens Vej 35
DK-2500 Valby
Tel.: +45 3319 3200
Fax: +45 3319 3218
E-mail: dt@datatilsynet.dk
www.datatilsynet.dk

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

4.1. Content of the notifications

The controller (in this case the Danish National Police) will – if not prevented by other interests cf. article 15 of Law Enforcement Directive - inform the data subject whether or not data relating to him/her is being processed in SIS.

4.2. Procedure to submit a complaint

The applicant can submit a complain to the Danish Data Protection Agency if the applicant is dissatisfied with a decision made by the Danish National Police concerning request to access or a decision made by the Danish Return Agency concerning request to correction or deletion of data.

If the applicant wishes to file a complaint, the applicant must provide the following information:

- a description of the nature of the complaint
- a copy of the decision or response that the applicant has received from the Danish National Police or the Danish Return Agency
- any other material that the applicant think is relevant to the complaint

The applicant can also use the Danish Data Protections complaint form:

- Complaint form.pdf (datatilsynet.dk)

5. References of the main national laws that apply

- Act No. 502 of 23 May 2018 on the Data Protection Act
- Act No. 410 of 27 April 2017 on the Law Enforcement Act

3.7. ESTONIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

For direct access:
Politsei- ja Piirivalveamet (Police and Border Guard Board)
Pärnu mnt 139, Tallinn, 15060
ppa@politsei.ee

For indirect access:
Andmekaitse Inspektsioon (Data Protection Inspectorate)
Tatari 39, Tallinn, 10134
info@aki.ee

2. How to make an individual request and what to include in it?

2.1. Who can submit a request
Request can be submitted by data subjects, legal guardians or persons with the power of attorney.

2.2. How the request should be submitted
There is no formal form for the request, nevertheless there are sample forms here and here (in Estonian) that could be filled in. The request should be in written form, preferably electronically.

2.3. Minimum information to be supplied

- A signed application must be submitted to request, correct or delete data entered in the Schengen Information System. The application must state the requester's name, date of birth, nationality and a copy of the identification document attached.
- Justification of the request when requesting deletion or correction of the data.

2.4. Documents to be supplied
- Copy of the identification document

2.5 Language regime
- The requests must be submitted in Estonian.
- In case the request is submitted in English, the controller responds to the applicant in Estonian.

2.6. Link to website where information on how to apply for information/correction/deletion

Please see more information on the websites of DPI and PBGB.

3. Contact details of the national data protection authority

Andmekaitse Inspektsioon (Data Protection Inspectorate)
Tatari 39, Tallinn, 10134
info@aki.ee

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

4.1. Content of the notifications

The controller (PBGB) will notify the requester in case there is no data in the national register, unless prevented by law.

4.2. Procedure to submit a complaint

In case the requester in not satisfied with the reply or does not get any reply from the controller within 30 days after sending the request, the requester has the right to lodge a complaint with the Data Protection Inspectorate or an administrative court. Filing a complaint with the Data Protection Inspectorate is free of charge. The complain form is found on DPI's website.

5. References of the main national laws that apply

- Isikuandmete kaitse seadus (Personal Data Protection Act)
- Haldusmenetluse seadus (Administrative Procedure Act)

3.8. FINLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The National Police Board
PO Box 1000 (Vuorimiehentie 3), 02151 ESPOO
+358 295 480181
kirjaamo.poliisihallitus@poliisi.fi

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject can submit a request, and he / she can bring along an assistant.

2.2. How the request should be submitted

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 form can be accessed here: Use of right of access (poliisi.fi)
Applicants will be told if their request cannot be granted immediately when they make the request. The controller will let the applicants know when and how they will be given access to their data.

2.3. Minimum information to be supplied

Personal identity code (or date and place of birth), family name (also previous family name), given names (also previous given names), contact information (address, phone number, email)
The police has templates for exercising the right of access. You do not need to use the templates, however, but can also prepare your own document. Whether you use the police's templates or draw up your own document, your request must specify which of your data you wish to access.

In case of request for data correction or deletion, the justification for the request: request need to contain enough detail about whose personal data are at issue, which data of the police you want rectified or erased, why you feel that the information in question is incomplete, inaccurate or incorrect in view of the purpose of the processing, and how you want the information in question changed.

2.4. Documents to be supplied

- Proof of applicant's identity (e.g. driving licence, identity card, passport (only accepted means of identification outside Finland)).

2.5 Language regime

The request can be made either in Finnish, Swedish or English.
The applicant is replied using the same language used to make the request.

2.6. Link to website where information on how to apply for information/correction/deletion
Data protection and processing of personal data - Police (poliisi.fi)

3. Contact details of the national data protection authority

The office of the Data protection Ombudsman
Street address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: PL 800, 00531 Helsinki, Finland
+358 29 566 6700
tietosuoja@om.fi
www.tietosuoja.fi

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

4.2. Procedure to submit a complaint

You can ask the Data Protection Ombudsman to check the lawfulness of your personal data and the way in which they are being processed if your right of access has been postponed, restricted or denied or if the controller refuses to comply with your request to correct inaccuracies, supplement, erase or restrict the processing of your data

5. References of the main national laws that apply

- Act on the Processing of Personal Data by the Police
- Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security
- Data Protection Act

Restrictions on the right of access

The right to access your data can be denied in certain circumstances. The right of access can be restricted when such a restriction, considering your rights, is necessary and proportionate to safeguard

- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,
- another official investigation, audit or other such procedure,
- public security,
- national security, or
- the protection of the rights of others.

3.9. FRANCE

1. Contact details of the body to which requests for access, correction or deletion should be addressed

In France, the right of access to the Schengen Information System (SIS) could be direct for specific categories of alerts, i.e. exercised in the first instance with the data controller. The Ministry of the Interior is the competent authority for requests for access to the SIS.

In all other cases, the SIS is considered to be a file that involves State security, the defence or public safety, and therefore the right of access can only be exercised indirectly through the Commission Nationale de l'Informatique et des Libertés (CNIL).

Direct access
Ministère de l'Intérieur - Direction Générale de la Police Nationale
Place Beauvau
75008 Paris

Indirect access
Commission nationale de l'informatique et des libertés (CNIL)
Service de l'exercice des droits et des plaintes 1 (SDP1)
3, place de Fontenoy
TSA 80715
75334 Paris cedex 07
+33153732222

1.5. Functional email address

https://www.cnil.fr/fr/demander-une-verification-sur-un-fichier-de-police-ou-de-renseignement

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every data subject may send a request for the right of access to the controller, the Ministry of the Interior in Paris.

The person concerned may appoint another person (such as a lawyer) to carry out in their name and on their behalf, the exercise of the rights conferred by the GDPR and the data protection directive under the conditions described in the mandate (Decree 2019-536 of May 29, 2019 taken for the application of Law No. 78-17 of January 6, 1978, Arts. 77 and 135).

For minors and adults unable to exercise their rights on their own, it is, depending on the case, the parents, the holder(s) of parental authority or the guardian who carry out the procedure.

2.2. How the request should be submitted

According to Articles 77 and 135 of Decree No. 2019-536, the applicant must prove their identity by any means. However, when the controller has reasonable doubts as to the identity of the person, it may request any additional information that appears necessary, including, when the situation so requires, a copy of an identity document bearing the signature of the owner.
The ministry considers that it cannot allow the exercise of rights of access to its processing without

serious justification of the identity of the applicant, therefore the production of a photocopy or a scan of an identity document is systematically required.
Decree No. 2019-536 provides that the person can exercise his/her rights by using digital identity data when this data is necessary and deemed sufficient by the controller to authenticate its users. An email address does not constitute a digital identity.
The Ministry of the Interior may accept the use of substantial or high level digital identities within the meaning of European regulation eIDAS No. 910/2014 of July 23, 2014, depending on the sensitivity of the request through the use of a very secure tool, such as the digital identity card.
In accordance with the provisions of decree no. 2015-1423 of 05/11/2015 relating to exceptions to the application of the right of users to contact the administration electronically (Ministry of the Interior in this case), **requests for the right of access to the SIS can only be made by post**.

In accordance with the provisions of decree No. 2019-536 of 29 May 2019 taken for the application of the law No. 78-17 of 6 January 1978, the data controller responds to the request submitted by the interested party within two months of receipt.
The deadline is suspended when the controller requests information necessary to identify the data subject or carry out the operations requested.

2.3. Minimum information to be supplied

- The information required is as follows: surname, first names, date of birth, nationality, sex. This information is provided on the basis of the production of a valid identity document.
- The concerned person sends their request for the right of access to the controller by post. There is currently no template for access requests
- Requests for access do not have to be motivated, as well as requests for rectification or deletion of an alert, even if the information provided by the applicant on his/her situation can facilitate the processing of the request.

2.4. Documents to be supplied

- The Ministry of the Interior considers that, as the controller for the SIS, it cannot allow the exercise of access rights without serious justification of the identity of the applicant. The production of a photocopy of an identity document is systematically required as proof of identity, with a legible photograph bearing the signature of the person concerned.
- Pursuant to Articles 77 and 135 of the aforementioned decree, the request may also be presented by a person specially authorized for this purpose by the applicant, if this person proves their identity and the identity of the principal, the mandate as well as of the duration and of the precise object thereof.
- The mandate must also specify whether the proxy can be made the recipient of the response or whether it must be sent directly to the concerned person.
- The decree implementing the Data Protection Act does not mention the need for a notarial document in support of the request for the right of access.

2.5 Language regime

- In accordance with the law of 4 August 1994 on the use of the French language and in accordance with Ordinance No. 2015-1341 of 23/10/2015, referred to in Article L. 111-1 of the Code of Relations between the Public and the Administration, the use of the French language is prescribed in exchanges between the public and the administration.
- The applicants can submit their request only in French.
- The controller responds to the applicant in French.

3. Contact details of the national data protection authority

Commission nationale de l'informatique et des libertés (CNIL)
3, place de Fontenoy

- Right of indirect access: in certain cases, the rights can only be exercised indirectly through the CNIL.
- Right of direct access: in the absence of a response from the data controller or a response that appears to be incomplete, the rights can be exercised through the CNIL.

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

4.1. Content of the notifications

When the request is processed by the CNIL, the Commission determines, in agreement with the data controller, which data should or should not be disclosed to the applicant with regard to the necessity to protect the purposes of the processing, State security, defence or public safety.

When the Ministry of the Interior, as data controller, objects to the disclosure of the results of the checks conducted by the CNIL, the Commission will only notify the applicant that the necessary verifications have been carried out.

The Commission's reply shall also mention the legal remedies available to the applicant. For requests relating to processing or parts of processing concerning State security, as is the case with the SIS, the mention of the legal remedies specifies that the matter may be referred to the Council of State.

If the applicant is the subject of an alert introduced by another Member State, the CNIL will seek the cooperation of the data protection agency of said State.

If the verifications give way to the suppression of the alert to which the applicant was subjected, this will be communicated to him/her providing that the data controller doesn’t object to it.

If the person in charge of the treatment has given his consent, content of the notifications (whether personal data concerning the data subject is contained in the SIS, what is it, why and for what purpose it has been entered, by which authority)

When there is an SIS alert on the person concerned, the response letter indicates the reason for the search, the action to be taken and the start and end dates of the alert's validity.

4.2. Procedure to submit a complaint

5. References of the main national laws that apply

- Data Protection Act, known as loi “informatique et libertés”, law No. 78-17 of 6 January 1978, modified.
- Decree No. 2019-536 of 29 May 2019 taken for the application of the data protection Act.

As mentioned above, in accordance with the law of 4 August 1994 on the use of the French language and in accordance with Ordinance No. 2015-1341 of 23 October 2015, referred to in Article L. 111-1 of the Code of Relations between the Public and the Administration, the use of the French language is prescribed in exchanges between the public and the administration.

The applicant can submit his or her request only in French.

3.10. GERMANY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Bundeskriminalamt
BdA 4 – Petenten
65173 Wiesbaden
Tel.: +49(0)611/55-0
Fax: +49(0)611/55-12141
E-Mail: ds-petenten@bka.bund.de

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Information from the SIS can be provided to data subjects, lawyers with power of attorney and legal guardians. Legal entities do not have the right to request information.

2.2. How the request should be submitted

The request can be submitted by e-mail or in written form. In addition, the Bundeskriminalamt (BKA, Federal Criminal Police Office) offers a contact form at the following address: https://www.bka.de/DE/KontaktAufnehmen/Kontaktinformationen/Buergerkontakt/buergerkontakt_node.html

2.3. Minimum information to be supplied

Requests for information must include at least the following information: name, surname, date of birth, nationality, gender, citizenship, address.

2.4. Documents to be supplied

Requests from data subjects must also include the following documents:

- informal request for information;
- a legible copy of a valid identification document.

In case of a representation by a lawyer, the following documents are required:

- informal request for information;
- a current power of attorney mentioning the request and signed by the person concerned or a lawyer's assurance of the existence of a power of attorney mentioning the request for data information;
- legible copy of a valid identification document;
- lawyer's assurance that the client is identical with the person concerned (holder of the identity document).

2.5 Language regime

According to the national legislation "(§23 of the Verwaltungsverfahrensgesetz - Federal Law on administration procedures) the official language is German. Communication in other official languages of the EU may be accepted upon availability.

2.6. Link to website where information on how to apply for information/correction/deletion

Further information can be found on the following website:
https://www.bka.de/DE/KontaktAufnehmen/AnfragenAuskunftserteilung/AuskunftserteilungSIS/auskunftserteilungSIS_node.html

3. Contact details of the national data protection authority

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Federal Commissioner for Data Protection and Freedom of Information
Graurheindorfer Straße 153
53117 Bonn
Phone: +49 (0)228-997799-0
E-Mail: poststelle@bfdi.bund.de
De-Mail: poststelle@bfdi.de-mail.de

Website: https://www.bfdi.bund.de/

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

4.1. Content of the notifications

With an information request, the person concerned or his legal representative receives information about the respective data stored in the SIS. The BKA is responsible for providing information from the SIS for Germany. If the access requirements are met, the BKA usually provides complete access to the information stored about the person concerned.

4.2. Procedure to submit a complaint

In individual cases, however, the right to information may be denied or restricted. In these cases, the following legal remedies are available:
a) Objection
Data subjects can object to rejected requests for information, rectification and deletion. The objection shall be addressed to the authority, which rejected the request.

b) Judicial protection:
If the BKA does not provide information within the deadline set in Article 12 (3) Regulation (EU) 2016/679, a lawsuit at the administrative court in Wiesbaden for the provision of the information can be filed.

c) Complaint relating to data protection law
If a request for information has been rejected, a data subject can contact the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (for contact details, see point 3). The supervisory authority is also available for questions regarding the procedure.

5. References of the main national laws that apply

Bundesdatenschutzgesetz (BDSG) - *Federal Data Protection Act* (https://www.gesetze-im-internet.de/englisch_bdsg/)

3.11. GREECE

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministry of Citizen Protection, Section of the International Police Cooperation Division at the Hellenic Police Headquarters
3rd S.I.RE.N.E.
4 P. Kanellopoulou Str., 10177 Athens
Telephone 210-6998263 & 210-6998262
Fax 210-6998264 & 210-6998265
Functional email address sirene@sirene.gov.gr

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, appointed lawyers with power of attorney, third party legally authorised, and legal guardians

2.2. How the request should be submitted

By postal mail and e-mail.
Link to online forms:
http://www.hellenicpolice.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=26982&Itemid=898&lang=EN.
There is no deadline for the submission of an application

2.3. Minimum information to be supplied

Personal data of the applicant : name, surname, father's name, date of birth, nationality, citizenship
A model form of application can be found in:
http://www.hellenicpolice.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=26982&Itemid=898&lang=EN (for access requests)
https://www.dpa.gr/sites/default/files/2021-05/SIS%20%ce%91%ce%99%ce%a4%ce%97%ce%a3%ce%97%20%ce%94%ce%99%ce%91%ce%93%ce%a1%ce%91%ce%a6%ce%97%ce%a3%202021_final.pdf
(for correction - deletion requests)

In case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion): Data subjects are invited to provide any evidence which, in the opinion of the person concerned, should be taken into account when delivering the judgment for deletion from the relevant lists (e.g. court judgments of acquittal, residence permit for children or spouse, attestations for the submission of supporting documents for the issuance of residence permits, provided that third-country nationals are registered in the relevant lists due to a previous illegal stay).

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, driver's licence)
- residence permit in case one has been issued already
- proof of granted power of attorney
- suitably legal authorisation document for third party representation

2.5 Language regime

The Police will normally examine requests in English in addition to Greek and reply to applicants in English if so requested.

2.6. Link to website where information on how to apply for information/correction/deletion

http://www.hellenicpolice.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=26982&Itemid=898&lang=EN
(for access requests)
https://www.dpa.gr/en/enimerwtiko/themes/large_databases/Schengen_SISII/datasubjectsrights

3. Contact details of the national data protection authority

Hellenic Data Protection Authority
Supervisory Authority
Address: Kifissias 1-3, P.C.115 23, Athens, Greece
Telephone: +30-2106475600
Functional email address contact@dpa.gr
Website: www.dpa.gr

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

4.1. Content of the notifications

If the alert was issued under Article 24 of SIS II Regulation, the applicant will be informed of the data relating to him.

If the alert was issued under Article 26 or Article 36 of SIS II Decision, 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 security grounds or in the investigation of particularly serious offences. Where an alert under Article 26 of SIS II Decision 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 II, the department which entered the data, and the length of time it is to be stored.

4.2. Procedure to submit a complaint

The national Personal Data Protection Authority checks that the SIS alert concerning the applicant is lawful and legitimate by means of examining the relevant documents supporting the decision of entering and/or maintaining the alert and will finally issue a decision on the lawfulness of the alert. Since in Greece, data subjects' rights are exercised directly before the controller i.e. the Hellenic Police, the Hellenic DPA will examine complaints on the rights of access – correction –deletion if the data subjects have addressed them before the controller and had not received a reply or the reply was unsatisfactory. Data subjects may submit a complaint in person, via postal mail and e-mail. They are also invited to fill in the relevant complaint form and submit any supporting documents for the examination of their complaint.
Details of the procedure and the relevant form can be found in:
https://www.dpa.gr/en/individuals/complaint-to-the-hellenic-dpa

5. References of the main national laws that apply

Law 4624/2019 - Official Gazette: (ΦΕΚ) A 137/29.08.2019, Ministerial Decree 4000/432- λα΄/ 17.10.2012 (Official Gazette B 2805/17.10.2012) as amended by Ministerial Decree 4000/4/32-ν/2017 on the criteria and the procedure for the registration and deletion of aliens to/from the National List of Unwanted Aliens

3.12. HUNGARY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

SIRENE Bureau of the National Police Headquarters
H-1139 Budapest, Teve utca 4-6.
Tel: +36 1 443 5861
Fax: +36 1 443 5815
sirene@nebek.police.hu

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Anyone who is interested in knowing whether or not their data has been recorded in the SIS, or wishes to correct or have inaccurate data deleted can submit a request. The person concerned must provide credible proof of his/her identity for authentication.

2.2. How the request should be submitted

Anyone who is interested in knowing whether or not their data has been recorded in the SIS, or wishes to correct or have inaccurate data deleted should contact any government office (http://www.kormanyhivatal.hu/hu), police station (http://www.police.hu/magyarendorseg/szervezetif) or any Hungarian Embassy or Consulate (http://www.kormany.hu/hu/kovetsegek-konzulatusok) and fill in a request for information form which is transferred to the SIRENE Bureau of the Hungarian National Police Headquarters.
Form for requesting information on the basis of Art. 26 of the Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System

2.3. Minimum information to be supplied

In the request for information form the following information are to be supplied: family name, surname, place and date of birth, gender, nationality, travel document No. (ID No), address/mailing address.

2.4. Documents to be supplied

The person concerned or his/her representative must provide credible proof of his/her identity and/or his/her authorisation.

2.5 Language regime

The request for information form is available in Hungarian and English.

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.police.hu/en/content/data-stored-in-the-sis
https://www.naih.hu/international-affairs-schengen-information-system

3. Contact details of the national data protection authority

Nemzeti Adatvédelmi és Információszabadság Hatóság
(National Authority for Data Protection and Freedom of Information)

The Hungarian National Authority for Data Protection and Freedom of Information has the authority to conduct an investigation or an administrative proceedings for data protection following requests submitted to her/him according to the relevant provisions (52-61.§) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act"). The Authority investigates the lawfulness of data processing and data transfer in connection with SIS II upon request or ex officio. If the data subject has doubts concerning the answer received from the SIRENE Bureau, or if no answer is received from the SIRENE Bureau, she/he may apply to the Hungarian National Authority for Data Protection and Freedom of Information.

Postal address: 1363 Budapest, Pf.: 9.
Office address: 1055 Budapest, Falk Miksa utca 9-11.
Tel. +36 (30) 683-5969
+36 (30) 549-6838
+36 (1) 391 1400
Fax: +36 (1) 391-1410
ugyfelszolgalat@naih.hu
https://naih.hu/

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

4.1. Content of the notifications

The SIRENE Bureau is obliged to inform the data subject what personal data concerning the data subject is contained in the SIS, why and for what purpose it has been entered, and to whom and for what purpose it has been transferred. The SIRENE Bureau has the right to refuse the request but is obliged to inform the data subject about the fact of and the reason for denial. Information may only be denied in the interest of national security, the prevention or prosecution of crimes, the safety of the execution of sentences, and the protection of the rights of others.

4.2. Procedure to submit a complaint

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/she may apply to the Hungarian National Authority for Data Protection and Freedom of Information.

5. References of the main national laws that apply

- Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act")
- Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System
- Government Decree No. 15/2013. (28/I) on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System.

The language of an administrative proceeding is Hungarian by law. However as a general rule nobody shall suffer damage or be discriminated by the fact he/she does not speak Hungarian. For the applicable rules and regulations concerning the language regime one should refer to the provisions of the Act CL of 2016 on the Code of General Administrative Procedure**.**

3.13. ICELAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Applications should be addressed to the SIRENE Bureau in Iceland, which is run by the National Commissioner of the Icelandic Police (NCIP).

The NCIP's contact details are the following:
Ríkislögreglustjóri/National Commissioner of the Icelandic Police
Skúlagata 21
105 Reykjavík
ICELAND
Att. SIRENE Bureau
E-mail: rls@rls.is

2. How to make an individual request and what to include in it?

The right of access is direct, which means that data subjects have to address a request for information, correction or deletion to the SIRENE Bureau, which decides whether or not to grant access.

2.2. How the request should be submitted

Special application forms can be filled in at local police stations in Iceland or at the NCIP premises. Decisions on the release of information are taken by the SIRENE Bureau.

Access can be requested outside of Iceland. Within the Schengen Area, authorities responsible for the quality of the information registered in SIS can be contacted. Outside the Schengen Area, a request can be addressed to an embassy or a consulate of any Schengen country.

2.5 Language regime

According to Icelandic law, Icelandic is the national tongue of Iceland and an official language. When answering requests regarding SIS from foreign nationals, however, English is generally used and, if necessary, an answer will be provided for in another language which the applicant understands.

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

In cases where an applicant has received a standard reply: "No information is registered/it is not permitted to disclose registered information", the SIRENE Bureau must instruct the applicant that he may appeal against this decision to the DPA.

The DPA's contact details are the following:

Persónuvernd/The Data Protection Authority
Rauðarárstígur 10
105 Reykjavík
ICELAND
E-mail: postur@personuvernd.is.

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

4.1. Content of the notifications

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."

4.2. Procedure to submit a complaint

5. References of the main national laws that apply

The main national laws applying are: Act No. 51/2021 on the Schengen Information System in Iceland and Regulation No. 112/2000 on the Schengen Information System in Iceland.

3.14. IRELAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

An Garda Síochána
Data Protection Unit,
Third Floor,
89-94 Capel Street,
Dublin 1,
D01 E3C6.
Ireland

Tel. +353 (01) 666 952
DataProtection@Garda.ie

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, solicitors representing data subjects and the legal guardians of data subjects.

2.2. How the request should be submitted

Requests for access can be made by submitting a Data Access Request Form (F20) to the An Garda Síochána Data Protection Unit
https://www.garda.ie/en/about-us/online-services/data-protection-foi-police-certificates/an-garda-siochana-f20-october-2019-.pdf

2.3. Minimum information to be supplied

Full name, previous or other name(s) date of birth, current address, previous address, phone number of the applicant;

2.4. Documents to be supplied

- A request in writing must be made and signed by the applicant.
- An acceptable form of proof of identity and proof of address must accompany the Subject Access Request form:
    - A copy of Photo ID i.e. Passport or Driving Licence and a copy of a recent Utility Bill or Government letter issued within the last six months to your current address.
- If the application is being made through a solicitor, a signed form consenting to the release of data to solicitor is required.
- Third party requests by parent/guardian requires their identification documents.

2.5 Language regime

The Data Access Request Form (F20) is requested to be completed by the data subject in English. Where necessary, additional translation services will be sought by the An Garda Síochána Data Protection Unit in relation to a request.

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.garda.ie/en/about-us/online-services/data-protection-foi-police-certificates/an-garda-

siochana-and-data-protection.html

3. Contact details of the national data protection authority

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland
Telephone +353 (0)1 7650100
Functional email address info@dataprotection.ie
Website: www.dataprotection.ie
https://forms.dataprotection.ie/contact

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

4.1. Content of the notifications

Following consideration of each request on a case-by-case basis, the content of the notifications may confirm/deny whether personal data concerning the data subject is contained in the SIS, a copy of the data may be supplied or restrictions invoked denying release of the data.

4.2. Procedure to submit a complaint

If the answer to a request is considered to be unsatisfactory, data subjects may lodge a complaint with the Irish data protection authority, the Data Protection Commission.

5. References of the main national laws that apply

Council Decision 2007/533/JHA
Data Protection Act 2018 (https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html)

Ireland's participation in SIS II is governed by Council Decision 2007/533/JHA.

The exercise of a data subjects right's is expressly provided for in Article 58 of Council Decision 2007/533/JHA.
Sections 90-95 of the Irish Data Protection Act 2018 outline the relevant provisions regarding the data subject's rights of information (90), access (91), rectification, erasure and restriction of processing (92), the obligations of the data controller regarding communication with the data subject (93), the available restrictions for data controllers on the exercise of rights (94) and the indirect exercise of rights and verification by the Irish data protection authority, the Data Protection Commission (95).
In response to access requests specific to SIS II, the An Garda Síochána Data Protection Unit will liaise with the national SIRENE Bureau.

In response to general access requests, data subjects are provided with a disclosure detailing relevant incidents and court outcomes held on Irish police systems concerning them - this would include any incidents created as a result of actions taken by the Irish police following a relevant SIS alert (provided no restriction is applicable to the disclosure).

The vast majority of Subject Access Requests processed by the An Garda Síochána Data Protection Unit are processed within the statutory timeframe of one month provided under Section 91(2) of the Data Protection Act 2018. This timescale can be extended by a further two months owing to the volume of requests received by the controller or the complexity of the request.

Requests for rectification or erasure are managed by the Data Protection Unit in line with similar timescales as provided under Section 92 of the Data Protection Act 2018 and the provisions of Article 58 of Council Decision 2007/533/JHA (i.e. normally within one month of receipt, with a provision to extend the timescale for consideration and action but no later than three months from the date of the request).

3.15. ITALY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministero dell'Interno -Dipartimento della pubblica sicurezza-Direzione centrale della polizia criminale - V Divisione - N.SIS
Via Torre di Mezzavia n. 9 00173 Roma
Telephone – not available
Fax + 39 06 46540950
dipps.dcpcsis.access@pecps.interno.it

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject, relatives (e.g. wife and husband), lawyer with power of attorney, legal guardian, third party (NGO).

2.2. How the request should be submitted

- in person, paper and/or electronic format, digitally or physically signed.
- link to online forms
- there is no deadline.

2.3. Minimum information to be supplied

- personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);
- use of model forms to exercise the rights vis-à-vis the SIS;
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion) in particular by showing the previous documents on it issued by the police authorities or the decisions of the judicial authorities.

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, residence permit, birth certificate);
- proof of granted power of attorney;
- notarial verified letter of attorney (in case of authorisation of representation by third party);.

2.5 Language regime

- For a quicker reply it is advisable that the same are written, if possible, in Italian, English, French or German. In any case, the data subject can use his own national language.

2.6. Link to website where information on how to apply for information/correction/deletion
https://www.gpdp.it/web/guest/schengen

3. Contact details of the national data protection authority

Garante per la Protezione dei dati personali
Supervisor Authority
Piazza Venezia 11 00187 Roma - Italy
Telephone - (+39) 06.696771
Fax - (+39) 06.69677.3785

Functional email address - protocollo@gpdp.it
Website - https://www.gpdp.it

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

In the event that a satisfactory answer is not provided to the request, the interested party can make a report or a complaint, without incurring any cost, to the Italian DPA

5. References of the main national laws that apply

Personal data protection code as amended by legislative decree No 101 of 10 August 2018 containing provisions to adapt the national legal system to Regulation (EU) 2016/679, and by legislative decree No 51 of 18 May 2018 containing provisions to adapt the national legal system to directive (EU) 2016/680. There are no specific provisions in place regarding processing of SISII data for police or migration purposes; accordingly, the provisions adopted to implement the Schengen Convention by way of Law No. 388/1993, ratifying and enforcing the protocols to the Schengen Convention, continue to apply insofar as they are not incompatible with SISII Regulation (UE) 2018/1861 and Regulation (UE) 2018/1862 which will enter into force on 7 March 2023

3.16. LATVIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

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

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

In accordance with Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 3.The data subject, by submitting an application, shall confirm his or her identity by providing a personal identification document. The authorised person shall present a notarily certified power of attorney that gives the right to receive information regarding the data subject or shall present a document that confirms the rights of parents, adopters, guardians or trustees. If the application is submitted electronically, the identity of the data subject shall be confirmed by a secure electronic signature.

2.2. How the request should be submitted

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.

2.3. Minimum information to be supplied

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.
https://www.dvi.gov.lv/lv/media/122/download?attachment

2.4. Documents to be supplied

Please see 2.3.

2.5 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.

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.vp.gov.lv/lv/sengenas-informacijas-sistema

3. Contact details of the national data protection authority

Data State Inspectorate of Latvia
National data protection authority
Elijas iela 17, Rīga, LV-1050
Phone:+371 67223131
pasts@dvi.gov.lv
https://www.dvi.gov.lv/

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

4.1. Content of the notifications

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.

Only restriction in national laws to provide answers to a data subject request is mentioned in Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 8. If the provision of the requested information is not authorised in accordance with the Law on Operation of the Schengen Information System or it is not kept in the Schengen Information System or the SIRENE information system, the answer with the following content shall be provided to the requester of the information: "There is no such information regarding you in the Schengen Information System and the SIRENE information system that you are entitled to receive on the basis of the duty to provide information specified in the Law on Operation of the Schengen Information System."

4.2. Procedure to submit a complaint

Procedure to submit a complaint is mentioned in Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 9. If it is refused to provide the requested information to the data subject or a person authorised thereof or an answer has been provided in accordance with Paragraph 8 of these Regulations, the data subject or a person authorised thereof has the right to submit a submission to the State Data Inspection regarding the necessity to examine whether the rights of the data subject specified in the Law have been followed.

5. References of the main national laws that apply

Law on operation of Schengen information system - https://likumi.lv/ta/id/159481-sengenas-informacijas-sistemas-darbibas-likums
Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information

System - https://likumi.lv/ta/en/en/id/164148-procedures-for-the-request-and-issue-of-information-regarding-a-data-subject-that-is-kept-in-the-schengen-information-system-and-the-sirene-information-system

3.17. LUXEMBOURG

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Requests for access should be addressed to the data protection officer of the Grand-Ducal Police of Luxembourg:

Direction Générale de la Police Grand-Ducale
A l'attention du **délégué à la protection des données**
Cité Policière Grand-Duc Henri,
B.P. 1007
L-2957 Luxembourg ,
Email : dpo@police.etat.lu

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

A request can be submitted either by the data subject or his/her attorney.

2.2. How the request should be submitted

The procedure is free of charge.
An identity verification procedure is however applied. Data subjects must proof their identity by sending to the Police a copy of an ID document. The access request procedure can by launched via letter or e-mail, both with a duly signed letter.
A request where one of these documents is missing is considered incomplete and will not be processed.

2.3. Minimum information to be supplied

- name and surname,
- nationality,
- date and place of birth,
- address.

Model letters (FR and EN) are provided on the website of the Grand Ducal Police.

In case a lawyer from abroad wishes to file a request, the following documents are required for a request to be considered complete:

- a power of attorney signed by the client and the attorney,
- a copy of an ID document of the client,
- a copy of an ID document of the attorney,
- a copy of an attorney card or equivalent.

2.4. Documents to be supplied

- a copy of an ID document of the data subject.

2.5 Language regime

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

- Luxembourgish;
- French;
- German;

- English.

2.6. Link to website where information on how to apply for information/correction/deletion

Data protection notice of the Grand Ducal Police containing a specific section on SIS (English version provided under the French version): https://police.public.lu/fr/support/protection-des-donnees-a-caractere-personnel.html

3. Contact details of the national data protection authority

Commission nationale pour la protection des données
15, boulevard du Jazz
L-4370 Belvaux
Website : https://cnpd.public.lu/en.html
Complaint form : https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html
Telephone : (+352) 26 10 60-1

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

4.1. Content of the notifications

The Grand Ducal Police has to provide an answer within 60 days.
If, in accordance with Article 41 (4) of Regulation 1987/2006 or Article 58 of Decision 2007/533/JHA (decision to not provide information to the data subject), and in the cases referred to in Article 12 (3) (delaying, restricting or omitting information to the data subject), Article 14 (1) (refusal or restriction of access to personal data) and Article 15 (4) (refusal of rectification or erasure of personal data) of the Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, the Grand Ducal Police has to inform the data subjects thereof, except for those cases where even the provision of that information may be restricted for the same reasons (article 12(3), 14(2), 15(4)).
In these cases, the rights of the data subjects may be exercised through the data protection authority, which will carry out all necessary verifications. The Grand Ducal Police has to inform the data subject of the possibility to exercise his or her rights through the National Commission for Data Protection or to seek judicial remedy.

The National Commission for Data protection informs the data subject at least that it has proceeded to all necessary verifications or a review. It further informs the data subject of his or her right to seek a judicial remedy.

4.2. Procedure to submit a complaint

Should the data controller not answer within the prescribed time, or should the data subject not be satisfied with the answer received, he/she can contact the National Commission by submitting the online complaint form. The form can also be printed and send to the National Commission in paper format.
All necessary information can be found on the website of the National Commission:
https://cnpd.public.lu/en/particuliers/faire-valoir.html

5. References of the main national laws that apply

Law of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters (implementing Directive (EU) 2016/680), in particular Articles 11, 12, 13, 14, 15, 16 and 17.
Link to the French version: https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a689/jo

Link to the English version: https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/loi-police-justice-en.pdf

Law of 1 August 2018 establishing the National Commission for Data Protection and the general rules on data protection.
Link to the French version: https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo
Link to the English version: https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/Act-of-1-August-2018-on-the-organisation-of-the-National-Data-Protection-Commission-and-the-general-data-protection-framework.pdf
Please note that only the original language version (French) is legally binding.

3.18. LIECHTENSTEIN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Landespolizei des Fürstentums Liechtenstein (National Police)
Polizeikommando
Gewerbeweg 4
Postfach 684
9490 Vaduz
+423 236 71 11
info@landespolizei.li

2. How to make an individual request and what to include in it?

2.2. How the request should be submitted

The application for access must be addressed to the National Police in writing. In case the application is filed by a lawyer or legal guardian power of attorney resp. legal guardianship needs to be provided.

2.3. Minimum information to be supplied

The applicant must provide proof of their identity. If the application not filed in person at the National Police Force and is the applicant not a resident of Liechtenstein, the applicant must provide a certified copy of his/her passport, which must be sent per mail.

2.5 Language regime

An application can be submitted in German or English

2.6. Link to website where information on how to apply for information/correction/deletion

Information on how to apply for access/correction/deletion can be found here: https://www.datenschutzstelle.li/internationales/schengendublin-1

3. Contact details of the national data protection authority

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz
Telefon: +423 236 60 90
E-Mail: info.dss@llv.li
www.datenschutzstelle.li

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

4.2. Procedure to submit a complaint

Generally, a reply is given within 30 days. In case a reply cannot be given within this period the applicant has to be informed. However, an answer has to be provided no later than 60 days after filing the application. If a data subject is notified about the refusal or limitation of provision of information, the data subject may exercise their right of access via the Data Protection Authority. The National

Police shall inform the data subject about the possibility of consulting the Data Protection Authority and the available legal remedies. The Data Protection Authority further informs the data subject of the possibility of judicial remedy

5. References of the main national laws that apply

- Art. 57 ff. Data Protection Act
- Art. 34g Act concerning the National Police Force (LGBl. 1989 Nr. 48);
- Art. 29 and 30 Ordinance on the Schengen Information System (SIS) and the SIRENE Office (LGBl. 2022 Nr. 306).

3.19. LITHUANIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Data subjects' requests for access, correction or deletion (direct access) in Lithuania should be addressed to the Ministry of 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: bendrasisd@vrm.lt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- data subject;
- representative of the data subject.

2.2. How the request should be submitted

The request can be submitted personally directly to the data subject or his/her representative upon arrival at the Ministry of the Interior of the Republic of Lithuania, by sending the request by mail or electronic means of communication. All requests submitted in writing, including by means of electronic communication, must be signed by the data subject who submitted the request or his/her representative. When submitting an application by means of electronic communication, a digital copy of the signed application must be submitted or the application must be signed with a qualified electronic signature that complies with the 2014 July 23 Regulation (EU) of the European Parliament and Council No. 910/2014 on electronic identification and electronic transaction reliability assurance services in the internal market, which repeals Directive 1999/93/EC. A copy of the data subject's valid passport or corresponding travel document shall be submitted together with the request submitted by mail or electronic means of communication. In the case of reasonable doubts about the identity of the data subject who submitted the request,for the purpose of identity verification, the data subject may be asked to submit a photo by post or electronic means of communication, in which the image of the data subject's face would be captured and clearly visible, together with the personal data of the data subject's valid passport or corresponding travel document a sheet with all the entries on this sheet and a photo of the person.

2.3. Minimum information to be supplied

- personal data of the applicant (surname(s) and first name(s), personal identification number (if he/she does not have a personal identification number, date of birth), place of residence, contact details (phone or email address));
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion).

2.4. Documents to be supplied

- proof of applicant's identity (a copy of the data subject's valid passport or corresponding travel document);
- proof of granted power of representative.

2.5 Language regime

- Requests for access, correction or deletion must be submitted in the official language of the state (Lithuanian). The reply to the data subject is given 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).

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.ird.lt/en/international-cooperation-1/the-schengen-information-system

3. Contact details of the national data protection authority

State Data Protection Inspectorate
L. Sapiegos str. 17 , LT-10315, Vilnius, Lithuania
phone +370 5 279 1455
email: ada@ada.lt
internet: www.vdai.lrv.lt

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 at least during the past year.

4.2. Procedure to submit a complaint

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. 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. Model letters for exercising data subjects' rights are in the following links:

1) https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97lteis%C4%97ssusipazintiLT2017.docx
2) https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97lteis%C4%97ssunaikintiLT2017.docx
3) https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97lteisesistaisytiLT2017.docx
4) https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordatainformationinSchengenSISII2017EN.docx
5) https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordatacorrectioninSchengenSISII2017.docx
6) https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordeletionofdatainShengenSISII2017.docx

5. 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

3.20. MALTA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The Malta Police Force
Address: Police Headquarters, St Calcedonius Square, Floriana FRN 1530
Telephone: 2122 4001
Fax: N/A
Functional email address: dpu.police@gov.mt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject, lawyer acting on behalf of the data subject and parent/legal guardian acting on behalf of a minor.

2.2. How the request should be submitted

The Malta Police Force facilitates the submissions of requests by providing a model form which can be accessed online: https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-(SIS).aspx

2.3. Minimum information to be supplied

- use of model forms to exercise the rights vis-à-vis the SIS

The data subject is requested to provide the following information when using the model form: name and surname, nationality, date of birth, ID card number, passport number and address.

- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

In the case where the data subject requests the rectification of his or her personal data, the data subject is requested to indicate which personal data are to be rectified and the reason(s) for rectification.

In the case where the data subject requests the deletion of his or her personal data, the data subject is requested to indicate which personal data are to be deleted and the reason(s) for erasure.

2.4. Documents to be supplied

The controller requests the following documents, where applicable: copy of passport, copy of the ID card and copy of the legal authorisation to represent the data subject.

2.5 Language regime

Maltese and English

2.6. Link to website where information on how to apply for information/correction/deletion

https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-(SIS).aspx

3. Contact details of the national data protection authority

Office of the Information and Data Protection Commissioner
The national supervisory authority responsible for the monitoring and enforcing the application of the data protection legislation.
Office of the Information and Data Protection Commissioner, Airways House, High Street, Sliema SLM1549
Telephone: +356 2328 7100
Fax: N/A
Functional email address: idpc.info@idpc.org.mt
Website: https://idpc.org.mt/

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

4.1. Content of the notifications

The data subjects shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of and legal basis for the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;
(f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
(g) communication of the personal data undergoing processing and of any available information as to their origin.

4.2. Procedure to submit a complaint

Pursuant to regulation 53(1) of Subsidiary Legislation 586.08, the data subject shall have the right to lodge a complaint with the Commissioner, if the data subject considers that the processing of personal data relating to him or her infringes the data protection regulations.
The Commissioner facilitates the submissions of complaints by providing a complaint submissions form which can be completed electronically on its website: https://idpc.org.mt/raise-a-concern/
This, however, does not exclude other means of communication insofar as the complaint is made in writing.

5. References of the main national laws that apply

Part III of the Data Protection (Processing of Personal Data by Competent Authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties) Regulations, Subsidiary Legislation 586.08 sets forth the rights of the data subjects.

In terms of regulation 15(1) of Subsidiary Legislation 586.08, the data subjects' rights may be restricted, wholly or partly, and for as long as such a partial and complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, for any of the following reasons:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

Regulation 15(2) of Subsidiary Legislation 586.08 states that the controller shall inform the data subject, without undue delay, and in no later than forty days from receiving the request, in writing of any refusal or restriction of access and of the reasons for the refusal of the restriction.

The languages of the requests and the replies should be in Maltese and English. Article 5(2) of the Constitution of Malta provides that “any person may address the Administration in any of the official languages and the reply of the Administration thereto shall be in such language".

3.21. NETHERLANDS

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Dutch National Police - Central Unit
Privacy Desk
PO Box 100
3970 AC Driebergen
Tel: +31 618 144 712
e-mail: jz.le@politie.nl

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Any individual or his or her (legal) representative or legal guardian (in case of a minor under the age of 16 or persons under guardianship) can submit an individual request.

2.2. How the request should be submitted

A request must be submitted in writing, or by completing the designated form on www.politie.nl via https://www.politie.nl/en/contact/forms/schengen-request-form.html?sid=ac78a8bc-d5f8-4e56-ab3b-aa85818fd529

Requests are made free of charge.
Once access to data has been provided, a subsequent request may be submitted for data to be rectified or erased. The applicant will be informed within 6 weeks after submitting the rectification or erasure request.

2.3. Minimum information to be supplied

Upon receiving a request for access, the Data Protection Officer must ensure that the identity of the data subject is properly established. If the Data Protection Officer has reason to doubt the identity of the data subject, additional information necessary to confirm the identity of the data subject may be requested.

2.4. Documents to be supplied

All requests must be accompanied by a valid proof of identity and the applicant's signature. A copy of the identity document must be provided and – where applicable – proof of legal authorisation to represent the applicant. Requests on behalf of minors or persons under guardianship must also be accompanied by proof of authorisation.

2.5 Language regime

- Requests may be submitted preferably in Dutch or English, but will also be accepted in French, German or Spanish.
- Requests will be replied to in Dutch, unless the request is made in English, French, German or Spanish. A reply in that case will be in English. Applicants using another language than Dutch should take additional time for translation into account.

2.6. Link to website where information on how to apply for information/correction/deletion

Schengen | politie.nl ; https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/europese-informatiesystemen

3. Contact details of the national data protection authority

Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
PO Box 93374
2509 AJ DEN HAAG
The Netherlands
Tel. +31-70-8888500
Fax +31-70-8888501
website www.autoriteitpersoonsgegevens.nl

Applications/complaints may be submitted in writing, or online via Complaint or request regarding the processing of personal data in the European information systems | Autoriteit Persoonsgegevens

The Dutch Data Protection Authority is the national supervisory authority responsible for supervision of the processing of personal data in N.SIS. The data subject may request the Dutch Data Protection Authority for mediation or advice in case of a dispute with the controller regarding the processing of a request for access to data, or a request for completion, rectification or erasure. An application must be submitted within 6 weeks of receipt of the controller's decision. The Dutch Data Protection Authority can also handle complaints lodged by a data subject, or by a body, organisation or association representing the data subject.

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

4.1. Content of the notifications

The data subject has the right to obtain from the controller confirmation as to whether or not personal data relating to them are being processed and, where that is the case, to access such personal data and to obtain information on:
a. the purposes and the legal basis of the processing;
b. the categories of police data concerned;
c. whether the data concerning that person have been provided throughout a period of four years prior to the request and on the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organisations;
d. the envisaged period of storage or, if that is not possible, the criteria for determining that period;
e. the right to request rectification, destruction or restriction of the processing of data relating to them;
f. the right to lodge a complaint with the Dutch Data Protection Authority, and the contact details of the authority;
g. the origin, to the extent available, of the processing of the data relating to them.

Within 6 weeks after submitting the request a reply must be communicated to the applicant.

4.2. Procedure to submit a complaint

If a data subject does not agree with the reply to his or her request for access, rectification or erasure, an appeal can be lodged with the administrative section of the District Court. Under Dutch administrative law, an appeal must be submitted within 6 weeks after the reply was sent to the applicant.
The data subject may also request the Dutch Data Protection Authority for mediation or advice in case of a dispute with the controller regarding the processing of his or her request for access, rectification or erasure. An application must be submitted within 6 weeks of receipt of the controller's decision.

If mediation by the Dutch Data Protection Authority has failed, an appeal may be lodged with the District Court to consider the case as it finds appropriate. Such an appeal may be filed after the interested party has received notification from the Dutch Data Protection Authority that the mediation case is closed, but in any event no later than 6 weeks after this notification. Without prejudice to existing means of redress, every data subject has the right to file a complaint with the Data Protection Authority if the data subject is of the opinion that the processing of personal data concerning them is unlawful. Complaints can be submitted in writing or by using the designated online form Complaint or request regarding the processing of personal data in the European information systems | Autoriteit Persoonsgegevens.

5. References of the main national laws that apply

The Police Data Act (Wet politiegegevens) and the Police Data Decree (Besluit politiegegevens) are applicable to personal data in case of law enforcement related SIS alerts. The GDPR is applicable to personal date in case of migration related SIS alerts.
The Dutch General Administrative Law Act (Algemene wet bestuursrecht) provides for administrative procedural rules with regard to decisions of administrative bodies and appeal procedures.
A request for access, rectification or deletion may be refused to the extent that this constitutes a necessary and proportionate measure, to avoid obstructing legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties; to protect public security or to protect the rights and freedoms of third parties.

3.22. NORWAY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Kripos
(National Criminal Investigation Service - NCIS)
PO Box 2094 Vika
NO-0125 OSLO
Tel.: +47 23 20 80 00
Fax: +47 23 20 88 80
E-mail: kripos@politiet.no
Internet: www.politiet.no

2. How to make an individual request and what to include in it?

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

2.1. Who can submit a request

A data subject or a person who presumes to be registered can submit a request, as well as a lawyer or other representative or legal guardian.

If the person listed in the database is younger than 15 years of age, the request must be signed by a parent or legal guardian. From the age of 15, listed persons can request access themselves under the Police Databases Act. Parents/legal guardians can, on their own initiative, request access to information about the listed person (the minor) until the minor reaches the age of 18. The minor should be informed of such requests.

Legal representatives or anyone requesting access on behalf of somebody else, must present a valid letter of authority.

2.2. How the request should be submitted

A request should be sutmitted in writing, either on paper or in an electronic format.
Link to online form: request-for-access-to-information-in-the-schengen-information-system-sis.pdf (politiet.no)

2.3. Minimum information to be supplied

- Name, address, postal code, city, country, date of birth, telephone number, e-mail address.
- Description of the information you request access to, seek to have corrected or deleted. In case of request for data correction or deletion, the justification of the request: e.g. the corrections required, description of circumstances, reasoning for the correction or deletion.
- Proof of applicant's identity.
- If you have a Norwegian national identity number or a central immigration system number, please state this.
- If you are represented by an agent, legal representative or other, please present a valid letter of authority.

The following are considered valid proof of identity:

- Valid passport (not emergency passport)
- Norwegian bank card with a photo
- Norwegian driving licence (not older versions – “green driving licence”)
- Nordic driving licence of EU/EEA standard
- The Ministry of Defence's ID card (from 2004)
- Valid Norway Post ID card issued after 1 October 1994
- National ID card issued in the EEA
- Asylum application registration card with signature and place of birth
- Norwegian refugee travel document (green passport)
- Norwegian immigrant's passport (blue passport)

2.4. Documents to be supplied

- Proof of applicant’s identity.
- Form for request provided by NCIS.
- If relevant, valid letter of authority.

2.5 Language regime

You may submit your request in English, Norwegian, one of the Sami languages, Swedish or Danish. The reply from Norwegian authorities will be in English or in Norwegian.

2.6. Link to website where information on how to apply for information/correction/deletion

Access to information in the Schengen Information system – Politiet.no

3. Contact details of the national data protection authority

Datatilsynet
PO Box 458 Sentrum
NO-0105 OSLO
Tel.: +47 22 39 69 00
Fax: + 47 22 42 23 50
E-mail: postkasse@datatilsynet.no
Internet: www.datatilsynet.no/en

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

In case there is an alert in the SIS, and as long as the information can be communicated to the data subject, the following information is provided to the applicant: kind of alert and for what purpose; Member State that introduced the alert; date of creation of the alert; other personal data processed in the SIS, including photograph, if applicable.

If the request (for data correction or deletion) is denied, the applicant is informed about the possibility to challenge this decision in the court.

4.2. Procedure to submit a complaint

A complaint to the Norwegian Data Protection Authority should be made in writing, either on paper or in an electronic format. There is no deadline to complain to the Norwegian Data Protection Authority.

Link to information on how to complain to the Norwegian Data Protection Authority: https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/

If your request has been denied by Norwegian authorities or your complaint has been dismissed by the Norwegian Data Protection Authority, you may challenge this decision before the courts of Norway.

Compensation

You may be entitled to compensation if you have suffered some harm because of the information recorded unlawfully in the database, or if information is used in a way that breaks the SIS rules. Please see the Norwegian Act relating to the Schengen Information System no. 6 of 18 February 2022 Section 19 and Section 20 and Regulation relating to the Schengen Information System no. 1194 of 26 June 2022 Section 2 and Section 3.

You must claim compensation no later than one year after you found out what information had been recorded. You can send your claim for compensation to Norway's NCIS or to the authority that decided the information should be recorded.

You may complain to the National Police Directorate or the Ministry of Justice and Public Security if your claim for compensation have been rejected.

5. References of the main national laws that apply

- Act relating to the Schengen Information System no. 66 of 16 July 1999 (LOV-1999-07-16-66). Link to Norwegian text: https://lovdata.no/lov/1999-07-16-66
- Regulation relating to the Schengen Information System no. 1194 of 26 June 2022 (FOR-2022-06-26-1194). Link to Norwegian text: https://lovdata.no/forskrift/2022-06-26-1194

3.23. POLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

1.1. Official name of the body to which a request for access should be addressed

Komendant Główny Policji (en. Commander-in-Chief of the Police)

1.2. Address

Central Technical Authority of the National IT System (CTA NITS)

National Police Headquarters

148/150 Puławska St.

02-624 Warsaw

Poland

1.3. Telephone

+ 48 47 72 148 79

+ 48 47 72 131 45

1.4. Fax

+48 47 72 129 21

1.5. Functional email address

The National Police Headquarters has launched an Electronic Inbox on the ePUAP platform. It enables the receipt and handling of electronic documents signed with a qualified electronic signature. Please note that in order to submit an application to the National Police Headquarters, it is necessary to have a free user account on the ePUAP platform. Electronic Platform of Public Administration Services (ePUAP) is a Polish nationwide platform for communication of citizens with public administrations in a uniform and standardized way. Built as part of the ePUAP-WKP project (State Informatization Plan). Service providers are public administration units and public institutions (especially entities that perform tasks commissioned by the state). Currently all administration services are available in Polish only.

http://bip.kgp.policja.gov.pl/kgp/elektroniczna-skrzynka/11424,Elektroniczna-skrzynka-podawcza.html

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every person has the right to:

- access to own personal data
- rectification of inaccurate own personal data
- erasure of personal data unlawfully processed

- file a complaint to the President of the Personal Data Protection Office

A person may be represented by a proxy, unless the nature of the act requires his / her personal action, in accordance with art. 32 of the Act of 14 June 1960, the Polish Administrative Code (Journal of Laws of 2022, item 2000, as amended).

Rules of giving legal proxy are set in art. 33 the Polish Administrative Code, i.e.:

- the proxy of a party can be natural person having legal capacity;
- the proxy should be submitted in writing;
- the proxy attaches to the file an original or officially certified copy of the proxy.

A lawyer or a legal/tax advisor and patent agent can certify a copy of a proxy given to them

2.2. How the request should be submitted

The application to Central Technical Authority of the National IT System (CTA NITS) - The Commander in Chief of the Police can be directed to:

- By post:

  Central Technical Authority of the National IT System (CTA NITS)

  National Police Headquarters

  148/150 Puławska St.

  02-624 Warsaw

  Poland

- via an electronic inbox available at: http://bip.kgp.policja.gov.pl/kgp/elektroniczna-skrzynka/11424,Elektroniczna-skrzynka-podawcza.html

Schengen-related requests received (also by e-mail) by the Protection Personal Data Protection Office - the national data protection authority - are forwarded, according to jurisdiction, to the National Police Headquarters.

2.3. Minimum information to be supplied

For this purpose, a written application should be submitted in Polish, which should obligatorily include:

a) name(s) and surname of the applicant;
b) citizenship;
c) date and place of birth (city and country);
d) address for return correspondence (country, city, postal code, poviat/area, voivodeship/district, street and house/apartment number) - in the case of an application sent by post;
e) the subject of the application;
f) handwritten signature of the person submitting the application.

Additionally, in order to unambiguously identify the data, the applicant may provide in the application:

a) previous/family name;
b) PESEL number (if the person has it);
c) sex;
d) place of residence (country, city, postal code, poviat/area, voivodeship/district, street and

house/apartament numer);

e) attach a photo copy of the page of the identity document containing personal data.

In case of doubts as to the identity of the person who submitted the application, the administrator may request additional information necessary to confirm the person's identity (Article 28 *Act d.p.c.c.* and Article 12 paragraph 6 *GDPR*).

The form which can be used to submit an application is available at: https://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188,The-right-of-data-subjects-to-information.html.

2.4. Documents to be supplied

- Written application.
- A copy of a valid identity document as defined by the national law of a Schengen State (passport/ID card/driving licence (other valid identity document);
- An original or officially certified copy of the proxy (in case of authorisation of representation by third party).

2.5 Language regime

In Poland, the official language is Polish, therefore all the applications must be submitted in Polish.

2.6. Link to website where information on how to apply for information/correction/deletion

- https://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188,The-right-of-data-subjects-to-information.html
- https://uodo.gov.pl/pl/479/2064

3. Contact details of the national data protection authority

3.1 Official name of the national data protection authority

Urząd Ochrony Danych Osobowych (en. Personal Data Protection Office)

3.2 Role

In order to provide an adequate level of legal protection for persons whose data is stored in the Schengen Information System, Personal Data Protection Office 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.

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

3.3 Address of the responsible body
Personal Data Protection Office
2 Stawki St.
00-193 Warsaw

Poland

3.4 Telephone

Telephone: +48 22 531 03 00

3.5 Fax

Fax: +48 22 531 03 01

3.6 Functional email address

kancelaria@uodo.gov.pl

3.7 Website:

http://www.uodo.gov.pl

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

4.1. Content of the notifications

The data subjects rights are exercised in the Republic of Poland on the basis of the provisions of the GDPR or on the basis of the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime, (depending on the purpose of data processing, e.g. category of alerts).

According to the Art. 15 (1) of the GDPR the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

According to of the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime the data subject shall have the right, on his request, to obtain from the controller whether his or her data are processed or, where they have been processed, the right to be informed of:

1) the purpose of and legal basis for their processing;

2) the categories of personal data and of the data which are processed;

3) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

4) the period during which the personal data will be stored or, where that is not possible, the criteria used to determine that period;

5) the possibility of applying to the controller for the rectification or erasure of personal data or restricting the processing of personal data relating to that controller;

6) the right to submit to the President of the Office or to any other supervisory authority on the basis of a separate complaint, in the event of a breach of the rights of the person as a result of the processing of his or her personal data, and of the data of the competent authority of the President or of the other supervisory authority;

7) source of data.

According to the Art. 23 of the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime the data subject shall, at his or her request, be entitled to have access to his or her own personal data. Having regard to the request for access to personal data, the controller shall make available or provide to the applicant a copy of, or a copy of such data, in an accessible form. The controller shall inform the data subject of the reasons for the refusal or restriction of access and of the possibility to lodge a complaint with the President of the Office in the event of a breach of the rights of the person as a result of the processing of his or her personal data. The controller shall document the factual or legal reasons for refusal or restriction of access. The President of the Office shall, on his request, be made available to this information.

4.2. Procedure to submit a complaint

Anyone who believes that his or her personal data protection rights have not been respected may lodge a complaint against the controller with the President of the Personal Data Protection Office. Complaints may be submitted in written or electronic form. The complaint shall be sent by electronic means through the Electronic Inbox of the President of the Office, after completing the FORM – i.e. "General letter to a public body" available on ePUAP2 portal. With regard to Schengen-related issues, the DPA handles complaints that are lodged by e-mail.

Each complaint must contain:

- name and surname and address of residence;
- indication of the entity against which the complaint is lodged (name/name and surname, and address of the seat/residence);
- a detailed description of the violation;

- your request, i.e. indication of what action you expect from the Personal Data Protection Office (e.g. erasure of data, fulfilment of the information obligation, rectification of data, limitation of data processing, etc.);

- handwritten signature;

It is important to attach evidence confirming the controller's incorrect action (e.g. correspondence with the controller, contracts, certificates). This will make it easier for the Office's staff to assess the case. Complaints which do not contain the name and address will not be further considered due to the impossibility of contacting the complainant.

Details of how to lodge a complaint to the President of the Personal Data Protection Office are available at: https://uodo.gov.pl/en/559/941.

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 (OJ 2021.1041 of 09.06.2021)**

  The Act defines the principles and method of implementation of the Republic of Poland's participation in the Schengen Information System and the Visa Information System, including the obligations and rights of the authorities to make entries and consult data contained in the Schengen Information System and the Visa Information System through the National Information System.

- **Act of 10 May 2018 on the Protection of Personal Data (OJ 2019.1781 of 19.09.2019)**
  This Act applies to the protection of natural persons in connection with processing of personal data within the scope defined in Article 2 and Article 3 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union L 119 of 04.05.2016, p. 1), hereinafter referred to as “Regulation 2016/679”.

- **Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime (OJ 2019.125 of 22.01.2019)**

  The Act sets out:

  1) the terms and conditions for the protection of personal data processed by competent authorities for the purpose of identifying, tracing, detecting and combating criminal offences, including threats to security and public order, and the exercise of pre-trial detention, penalties, disciplinary sanctions and coercive measures for deprivation of liberty;
  2) rights of data subject processed by the competent authorities for the purposes referred to in point 1 and their remedies;
  3) the method of keeping of the supervision of the protection of personal data processed by the competent authorities for the purposes referred to in point 1, excluding data processed by the prosecution and the courts;

4) the tasks of the supervisory authority and the form and manner of their implementation
5) the obligations of the controller and of the processor and of the data protection officer and the procedure for its designation;
6) preservation of personal data;
7) procedures for cooperation between supervisory authorities in other Member States of the European Union;
8) criminal liability for failure to comply with the provisions of this Act.

- **Act of 14 June 1960, Code of Administrative Procedure (OJ 2022.2000 of 27.09.2022)**

  The Code of Administrative Procedure shall govern proceedings: 1) before public administration bodies in cases that are within the jurisdiction of such bodies and individually decided by way of administrative decision.

- **Act of 7 October 1999 on the Polish Language (OJ 2021.672 of 12.04.2021)**

  The provisions of the Act concern use of the Polish language in the implementation of public tasks.

3.24. PORTUGAL

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Gabinete Nacional SIRENE / SIRENE Bureau
Av. Defensores de Chaves, 6, 1049-063 Lisboa, Portugal
+351. 217 822 000
sirene.portugal@sef.pt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- Any individual;
- The applicant can be represented by a lawyer with powers of attorney, which should expressly mention in the mandate the exercise of the data protection rights;
- In case of a minor, the exercise of the rights can be performed by the respective legal representative.

2.2. How the request should be submitted

- in person;
- by post mail. (Not admissible requests by email).

2.3. Minimum information to be supplied

- Personal data of the applicant (name, surname, nationality, date of birth, place and country of birth; parents' name and surname, if applicable; passport or ID card number, date of issuance and expiry, issuer body; number of residence permit, issuance and validity date)
- Contact details (postal address, telephone, email)
- use of model forms to exercise the rights vis-à-vis the SIS, available for download in the organisation website in PT and EN versions.
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- readable certified copy of ID or passport, and of residence permit, if applicable
- proof of granted power of attorney, duly signed by the applicant (original)
- in case of minors, proof of legal representation by parents or others holding parental responsibility (original or certified copy).

2.5 Language regime

- what language(s) can be used to submit the request: Portuguese. (The model forms are available in English to assist fulfilment of the request).
- what language is used to reply to the applicant: Portuguese.

2.6. Link to website where information on how to apply for information/correction/deletion

PT version: https://www.puc-spoc.pt/direitos-schengen

EN version: https://www.puc-spoc.pt/en/schengen-rights

3. Contact details of the national data protection authority

Comissão Nacional de Proteção de Dados (CNPD)
Av. D. Carlos I, 134, 1.º, 1200-851 Lisboa, Portugal
Tel. +351. 213.928.400
Fax: +351.213.976.832
geral@cnpd.pt
https://www.cnpd.pt/

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

4.1. Content of the notifications

In case there is an alert in the SIS, and as long as the information can be communicated to the data subject, the following information is provided to the applicant: kind of alert and for what purpose; Member State that introduced the alert; date of creation of the alert and data of its actual validity; other personal data processed in the SIS, including photograph and fingerprints, if applicable.

Depending on the specifics of the request and of the case, further information can be communicated to the applicant (e.g. authority requesting the creation of the alert; facts and legal reasoning for the alert; ongoing consultations between competent authorities of Member States).

If the request (for data correction or deletion) is denied, the applicant is informed about the possibility to challenge this decision in the court.

4.2. Procedure to submit a complaint

Complaints should be submitted through a specific form available in the CNPD's website.
https://www.cnpd.pt/cidadaos/participacoes/geral/

5. References of the main national laws that apply

- Decree-Law 122/2021, of 30 December
- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)
- Law 59/2019, of 8 August .

3.25. ROMANIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Centre for International Police Cooperation - SIRENE Bureau
1-5 Calea 13 Septembrie, Bucharest, 5th District
Tel: +40 21 315 96 26; +40 21 314 05 40
Fax: +40 21 314 12 66; +40 21 312 36 00
ccpi@mai.gov.ro

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- data subject, lawyer with power of attorney, legal guardian

Persons whose personal data are collected, held or otherwise processed in the SIS II are entitled to rights of access, correction of inaccurate data and deletion of unlawfully stored data.

2.2. How the request should be submitted

- by regular post, by email.

2.3. Minimum information to be supplied

- personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- proof of granted power of attorney
- notarial verified letter of attorney (in case of authorisation of representation by third party)

2.5 Language regime

- . the request can be submitted in Romanian or English
- - the reply will be in Romanian or English, depending on the language used for submitting the request

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.dataprotection.ro/index.jsp?page=schengen&lang=en

3. Contact details of the national data protection authority

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
28-30 Gheorghe Magheru Blvd, 1st District, Bucharest
Tel: +40.318.059.211
Fax: +40.318.059.602
anspdcp@dataprotection.ro
www.dataprotection.ro

Pursuant to Article 64 of Law no. 141/2010, republished, the legality of the processing of personal data in N.SIS on the territory of Romania and the transmission of this data abroad, as well as the exchange and further processing of additional information are monitored and subject to the control of the National Supervisory Authority for Personal Data Processing (ANSPDCP).

In case the data subject does not receive a reply to his/her request for exercising the rights or is not satisfied with the answer received, he/she has the right to submit a complaint to ANSPDCP.

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

4.2. Procedure to submit a complaint

Right of access
The right of access is the possibility for anyone who so requests to have knowledge of the information relating to him or her 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 Article 53 of Regulation (EU) 2018/1861 and in Article 67 of Regulation (EU) 2018/1862.

The right of access is exercised in accordance with Law no. 141/2010, republished. Thus, pursuant to Article 62 of Law no. 141/2010, republished, the requests of the data subjects in the context of personal data processed in the NISA or the SIS can be submitted only to the national SIRENE Bureau which will communicate the answer to the applicant as soon as possible but no later than 60 days after the receipt of the request.

The requests may be submitted to the national SIRENE Bureau or to any data controller within the Minister of Internal Affairs or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

In the case of alerts entered in the SIS by another Member State, the requests of the persons are answered by the national SIRENE Bureau only with the consent of the Member State that entered the alert. The national SIRENE Bureau requests the consent through the exchange of supplementary information.

The data subject shall not be communicated information regarding personal data processed in SIS as long it is necessary for performing the activities on the basis of the alert or the objective of the alert or for protecting the rights and freedom of other persons.

Right to rectification and deletion of data
Besides the right of access, there are also the right to obtain the correction of personal data factually inaccurate or incomplete or the right to ask for deletion of personal data unlawfully stored (Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862).

Under the Schengen legal framework only the Member State responsible for issuing an alert in the SIS may alter or delete it (See Article 44(3) of Regulation (EU) 2018/1861 and Article 59(3) of Regulation (EU) 2018/1862.

The right of rectification and deletion of data is exercised in accordance with Law no. 141/2010, republished. Thus, pursuant to Article 62 of Law no. 141/2010, republished, the requests of the data subjects in the context of personal data processed in the NISA or the SIS can be submitted only to the national SIRENE Bureau which will communicate the answer to the applicant as soon as possible but no later than 90 days after the receipt of the request.

The requests may be submitted to the national SIRENE Bureau or to any data controller within the

Minister of Internal Affairs or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

If the request is submitted in a Member State that did not issue the alert, the competent authorities of the Members States concerned cooperate to handle the case, by exchanging information and making the necessary verifications.

5. References of the main national laws that apply

- Law no. 141/2010 on the setting up, organisation and functioning of the National Information System for Alerts and participation of Romania to the Schengen Information System, republished
- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

3.26. SLOVAK REPUBLIC

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministerstvo vnútra Slovenskej republiky (Ministry of Interior of the SR)
Prezídium Policajného zboru
Úrad medzinárodnej policajnej spolupráce
Národná ústredňa SIRENE
Pribinova 2
812 72 Bratislava
Slovenská republika
sirene@minv.sk

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

The request can submit any individual or deputy of the individual (a person authorised by data subject with the procuration).

2.2. How the request should be submitted

Written request shall be submitted

- in person, by post or electronically signed with electronic signature to the address of the Ministry of Interior of SR
- by email,
- by standard application form available on the website of the Ministry of Interior of SR

In Slovak
https://www.minv.sk/?Prava
In English
https://www.minv.sk/?Data-Subjects-Rights

Deadline: The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

2.3. Minimum information to be supplied

The data subject is obliged to provide his/ her personal data (name, surname, address of permanent residence, 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. If data subject is not a Slovak national, a colour copy (scan) of another document proving name and surname or changes of name/surname during your entire life (birth certificate, marriage certificate). Delivery address or email - depending on by which means the data subject wants an answer.

Forms:

- Request for provision of information on personal data processed in the Schengen Information System 2018 (RTF, 74 kB)
- Request for rectification of incorrect or outdated personal data processed in the Schengen Information System (RTF, 75 kB)

- Request for destruction of illegally processed personal data in the Schengen Information System (RTF, 74 kB)

In case of request for data correction or deletion, the applicants are informed to justify their request (identification of the object and proving relation to it).

2.4. Documents to be supplied

A copy of the applicant ID card or passport for the purpose of proving his/her identity. If data subject is not a Slovak national, a colour copy (scan) of another document proving name and surname or changes of name/surname during your entire life (birth certificate, marriage certificate). Document stating parental relationship (concerning request for a child).

If request is sent through a person authorised by data subject, it is required to attach the copy of the procuration to the request translated into English or Slovak language and certified by a notary.

2.5 Language regime

Slovak or English.

2.6. Link to website where information on how to apply for information/correction/deletion

In Slovak
https://www.minv.sk/?Prava

In English
https://www.minv.sk/?Data-Subjects-Rights

3. Contact details of the national data protection authority

Úrad na ochranu osobných údajov Slovenskej republiky
(Office for Personal Data Protection of the Slovak Republic, "Office")
Hraničná 12, 827 07 Bratislava 27, Slovenská republika (Slovak Republic)
Tel: +421 2 3231 3214
Fax: +421 2 3231 3234
statny.dozor@pdp.gov.sk
https://dataprotection.gov.sk/uoou

The Office is a state administration body with national jurisdiction over the territory of the Slovak Republic that participates in the protection of fundamental rights of natural persons in relation to processing of personal data and executes data protection supervision, including supervision of personal data protection by competent authorities for performance of the task for the purposes of criminal proceedings

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

4.1. Content of the notifications

The notification contents information about the data subject, what data, why and for what purpose and also by whom it has been entered. If the record contains photographs or dactyloscopic data of the person, data subject is informed that the record also contains this data. The notification contains also information that the data is accurate, actual and processed in compliance with the applicable laws. It contains also information on lodging the complaint with regard to data protection.

4.2. Procedure to submit a complaint

The right to lodge a complaint referred to as a request for verification of processing shall apply to the Office if the data subject (individual) considers that his or her data is being processed unlawfully in the relevant national component of the SIS. The Office is competent to review personal data processing within the national part of the SIS in case where there is suspicion of an unlawful procedure or a satisfactory response was not provided. According to the sec. 100 para. 3 of the Act. No. 18/2018 Coll. the complaint shall contain:

- **the name, surname, correspondence address and signature of the complainant,**
- **identification of the entity against which the complaint is addressed,** name, surname, permanent residency or organization name, headquarter and identification number if such number was assigned,
- **the subject of the complaint,** identifying the rights that might have been infringed during personal data processing,
- **evidence** supporting the arguments stated in the complaint,
- **copy of document or other type of evidence demonstrating the exercise of a right pursuant to second title of second chapter of the Act. No. 18/2018 Coll. or the Regulation 2016/679** if you have exercised such right, **or the reasons worth special consideration** if you have not exercise such right.

The complaint shall be submitted in Slovak language (the official translation is not required). The template of the complaint can be found **here. This template serves only for the information about the content requirements of the complaint.** In accordance with the Act No. 270/1995 Coll. on the State Language of the Slovak Republic the public authorities and the natural persons are obliged to use the state language – Slovak in the official communication. The proceeding is performed and the decisions are issued exclusively in Slovak language.

5. References of the main national laws that apply

- Act No. 18/2018 Coll. on personal data protection and amending and supplementing certain Acts
- Civil Code No. 64/1964 Coll. (section 22 – 33b provisions on representation)

3.27. SLOVENIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Policija, Ministrstvo za notranje zadeve
Štefanova 2
1501 Ljubljana
Slovenia
Tel.: + 386 1 428 45 75
Fax: + 386 1 428 47 33
E-mail: uit@policija.si

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Everyone has the right to request the review of relevant personal data entered in the SIS. Everyone has the right to request the correction of substantially incorrect data or the deletion of illegally obtained data entered into the SIS pertaining to him/her.

2.2. How the request should be submitted

Verbal confirmation and information given in Slovenia shall be free of charge, and any other services may only be charged according to an existing price list.

Requests can be filed in written form or also orally, for the record. Requests 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.

2.3. Minimum information to be supplied

Minimum information to be supplied: first name, last name, address, date of birth, place of birth, nationality.

2.4. Documents to be supplied

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: https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva%20za%20seznanitev%20s%20podatki%20v%20Schengenskem%20informacijskem%20sistemu%20v%20SI.docx

Persons who are not citizens of Slovenia must also attach a copy of a valid official document with a photo (ex. passport or ID) to this form.

2.5 Language regime

Requests may be submitted in English and Slovene language.

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

Informacijski pooblaščenec

(Information Commissioner)
Dunajska 22
1000 Ljubljana
Slovenia
Tel.: + 386 1 230 97 30
E-mail: gp.ip@ip-rs.si
Website: www.ip-rs.si

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

4.1. Content of the notifications

The process of exercising the right to consult one's own personal data in Slovenia is regulated in accordance with the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (Article 24) and the Information Commissioner Act.

Article 24 of the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences requires the Police, which is subordinate to the Ministry of the Interior and a data controller, to notify the individual whose personal data is processed about:
1. processing purposes and their legal basis;
2. types of personal data that are processed;
3. users or categories of users to whom data has been disclosed, especially if they are users in third countries or international organizations, and in cases of restrictions from the first paragraph of Article 25 of this law, only a rough description of the users may be provided;
4. the retention period of the period for regular review of the need for retention;
5. the existence of the right to request correction or deletion of data or restriction of processing and the right to file a complaint with the supervisory authority;
6. the existence of the right to file a report with the supervisory authority and its contact information;
7. all available information about the source of personal data, unless the identity of the source is protected as secret or confidential according to the provisions of the law.

The competent authority shall decide on the request without undue delay, but no later than one month after receiving the request.

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

4.2. Procedure to submit a complaint

Applicants who consider that any of their rights have been violated in relation to the request 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. References of the main national laws that apply

- The Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (Official Gazette of the Republic of Slovenia, no. 177/2020), unofficial English translation of the Act available at: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO8157#
- Information Commissioner Act (Official Gazette of the Republic of Slovenia, no. 113/2005, 51/2007 – ZUstS-A), unofficial English translation of the Act available at: https://www.ip-rs.si/en/legislation/information-commissioner-act/

3.28. SPAIN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

DIVISIÓN DE COOPERACIÓN INTERNACIONAL – OFICINA SIRENE

Avda. Pío XII, 50

28016 Madrid

2. How to make an individual request and what to include in it?

The procedure is free. Any request for access must be submitted in writing together with:

• Request right of access to SIS, the format can be found in the following links:

- Application Form for the Exercise of the Right of Access SIS Document in pdf. Formulaire de Demande pour l'Exercice du Droit d' Accès au SIS pdf document.

https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/extranjeria/acuerdo-de-schengen/sistema-de-informacion-de-schengen/sis_derecho_acceso_es_en.pdf

División de Cooperación Internacional (policia.es)SIS Rights of Access Application Form (policia.es)

Formulario de solicitud de derecho de acceso al SIS (policia.es)

https://www.policia.es/miscelanea/dci/formulaire_SIS.pdf

División de Cooperación Internacional (policia.es)SIS Rights of Access Application Form (policia.es)

Formulario de solicitud de derecho de acceso al SIS (policia.es)

• Copy of valid and valid identity document of the applicant, in which he can be fully identified.

• In case of exercising the right of access through a legal representative, in addition to the above, it will be required:

- Copy of valid and valid identity card of the representative, in which he can be fully identified.
- Document of authorisation of legal representation.

• Applications must be made through one of the following two ways:

- Submit the corresponding request addressed to:

General ADDRESS OF THE POLICY, INTERNATIONAL COOPERATION DIVISION, OFFICE SIRENE ESPAÑA,
Avda. Pio XII No. 50, 28016, MADRID

- An Electronic Registry through the SARA platform (Systems of Applications and Networks for Spanish Public Administrations and European Institutions) addressed to the address mentioned above, being necessary to be the holder of a Spanish identity document, whether it is National Identity Document, Passport or Foreigner Identity Card.

Interested parties who wish to submit a complaint related to the right of access to the Spanish Data Protection Agency can use the following link: https://www.aepd.es/es/internacional/supervision-de-grandes-sistemas/sistema-de-informacion-schengen-sis

2.1. Who can submit a request

- categories of applicants that can submit a request (data subject, lawyer with power of attorney, legal guardian)
- representation

Everyone has the right to exercise his or her right to know if there is information about him or her contained in the SIS, which is known as the *"exercise of the right of access*".

2.2. How the request should be submitted

- in person, paper and/or electronic format digitally signed (via the official electronic registry)

- link to online forms: https://www.aepd.es/en/international/supervision-of-large-systems/information-system-schengen-sis
https://www.policia.es/miscelanea/dci/formulario_sol_ejercicio_derecho_acceso_SIS.pdf
https://www.policia.es/miscelanea/dci/SIS_rights_of_access_application_form.pdf
https://www.policia.es/miscelanea/dci/formulaire_SIS.pdf

- deadline to submit information: one month

2.3. Minimum information to be supplied

- personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);

- use of model forms to exercise the rights vis-à-vis the SIS

- copy of the documents that proves the applicant's identity.

- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- proof of applicant's identity (e.g., readable copy of ID, passport, residence permit, birth certificate)

Name: Surname: Nationality: Date of birth: Identity card no. / Passport (a copy is attached): Full address:

- proof of granted power of attorney (in case of the right of access being exercise through a qualified lawyer)

- notarial verified letter of attorney or apud acta (in case of authorisation of representation by third party)

2.5 Language regime

***-** what language(s) can be used to submit the request: English, Spanish. French*

- what language is used to reply to the applicant: Spanish.

2.6. Link to website where information on how to apply for information/correction/deletion

https://www.aepd.es/en/international/supervision-of-large-systems/information-system-schengen-sis

https://www.policia.es/_es/tupolicia_conocenos_estructura_cooperacioninternacional.php

3. Contact details of the national data protection authority

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

Subdirección General de Inspección.

Jorge Juan 6, 28001-MADRID

Telephone +34 900 293 183

Functional email address

Website https://www.aepd.es › es

https://sedeagpd.gob.es/sede-electronica-web/https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/identificacionSolicitante.jsf

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

4.1. Content of the notifications

whether personal data concerning the data subject is contained in the SIS, what is it, why and for what purpose it has been entered, by which authority.

4.2. Procedure to submit a complaint

1) confirmation of the existence of information within the system.

2) The right of access to the "Schengen Information System" is freely provided within the maximum period of one month, starting from receipt of this request,

The information shall be sent by mail to the above address within the period of ten days from the date that this request for access is granted. Furthermore, that this information shall be legible and understandable, and will include the basic data included in the Schengen Information System files from any procedure, process, or processing, as well as their source, the transferees and details of the specific uses and purposes for which they are stored.

3) the right of access can be denied in accordance with art. 24 of the national Act transposing Directive 680/2018.

5. References of the main national laws that apply

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales: https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806
Those contained in art. 24 of the Spanish Organic law 7/2021 for the prevention, detection, investigation and prosecution of criminal offences or execution of criminal penalties

3.29. SWEDEN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Polismyndigheten
Noa/IE
SE-106 75 Stockholm
SWEDEN
registrator.kansli@polisen.se

2. How to make an individual request and what to include in it?

2.2. How the request should be submitted

You are entitled to be informed whether you are registered in the SIS, unless secrecy applies. You can also make a request for deletion or correction of information which is legally or factually incorrect.

The request to be informed whether you are registered in SIS must be made in writing and signed by you, the person requesting the information. A power of attorney is not accepted (other than in exceptional cases).

2.3. Minimum information to be supplied

Please provide your name, date of birth and postal address as the Police Authority may need to send the reply by post.

2.4. Documents to be supplied

A photocopy of a valid identity document must be attached to the request, unless you indicate that the reply should be sent to your registered address in Sweden.
Forms for the request are available on the Swedish Police website:
https://polisen.se/en/services-and-permits/police-record-extracts/schengen-information-system-sis--request-information/
2.5 Language regime

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

Integritetsskyddsmyndigheten
Box 8114
SE-104 20 Stockholm
SWEDEN

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

4.1. Content of the notifications

4.2. Procedure to submit a complaint

Application for withdrawal of a re-entry ban
If a person has been refused entry or deported with a ban on re-entry (applicable to non-EU citizens) and wishes to apply for withdrawal of the re-entry ban, the Swedish Migration Board should be

contacted. It is the Migration Agency, or a Migration Court, which examines an application for withdrawal of a re-entry ban.
The application for withdrawal of a re-entry ban should be sent to:
Migrationsverket
SE-601 70 Norrköping
SWEDEN

Complaint to the national supervisory authority, IMY
If you want to exercise your rights, you should first turn to the Police Authority who is the authority in Sweden responsible for personal data processing in the SIS II. If you are not satisfied with how your request has been dealt with by the Police Authority, you have the right to submit a complaint to the IMY.
How to contact IMY
Phone number: +46 (0)8 657 61 00
E-mail: imy@imy.se
Website: https://www.imy.se/en/organisations/data-protection/dataskydd-pa-eu-niva/eus-informationssystem/the-schengen-information-system/

Integritetsskyddsmyndigheten
Box 8114
SE-104 20 Stockholm
SWEDEN

3.30. SWITZERLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Federal Office of Police (fedpol)
Legal department/ Data protection
Data Protection Officer
Guisanplatz 1A
CH-3003 Berne
kpr-ks@fedpol.admin.ch

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

A data subject, lawyer with power of attorney or legal guardian, shall submit a request.

2.2. How the request should be submitted

Fedpol provides the opportunity to apply for information via Internet site:

- I am submitting the application for myself (admin.ch)
- I am submitting the application for someone else (admin.ch)

2.3. Minimum information to be supplied

The request shall usually be sent in writing in paper or electronic format.
Applicants do not need to justify their request for access. In case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion) has to be mentioned and the proof has to be enclosed.
The personal data (name, surname, personal address, date of birth, nationality, gender, citizenship) of the applicant has to be mentioned.
Model forms are available here:
https://www.edoeb.admin.ch/edoeb/en/home/data-protection/dokumentation/model-letters/schengen-and-your-personal-data.html

2.4. Documents to be supplied

The identity has to be proven by a copy of the applicant's valid passport.

2.5 Language regime

Requests can be transmitted in French, German, Italian or English.

2.6. Link to website where information on how to apply for information/correction/deletion

Further information is available here.

3. Contact details of the national data protection authority

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH-3003 Berne
Telephone: +41(0)31 322 43 95

Fax +41(0)31 325 99 96
Contact form via website: https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/kontaktformular.html
https://www.edoeb.admin.ch/edoeb/en/home.html

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

4.1. Content of the notifications

Content of the notifications whether personal data concerning the data subject is contained in the SIS

4.2. Procedure to submit a complaint

In case that fedpol does not respect the individual's access request she/he can submit a complaint to the Federal Data Protection and Information Commissioner (FDPIC). The FDPIC shall open an investigation upon notification against the federal body if there are indications that a data processing operation may violate the data protection provisions. The FDPIC may refrain from opening an investigation if the breach of the data protection provisions is of minor importance. If the person concerned has filed a complaint, the Commissioner shall inform him or her of the steps taken on the basis of this complaint and the result of any investigation (Art. 22 SADP, RS 235.3 [applicable until 31.8.2023], afterwards Art. 49 of the new DSG will be applicable).
The person can also appeal to the Federal Administrative Court in accordance to Art. 48 – 53 Administrative Procedure Act, APA).

5. References of the main national laws that apply

- Federal Act of 28 September 2018 on Data Protection in application of the Schengen acquis in criminal matters (SADP, RS 235.3; DE; FR; IT)
- Federal Act of 19 June 1992 on Data Protection (FADP; RS. 235.1)
- Ordinance of 14 June 1993 to the Federal Act On Data Protection (OFADP; RS. 235.11)
- Ordinance on the National Part of the Schengen Information System (N-SIS) and on the SIRENE Bureau (N-SIS Ordinance; RS. 362.0; DE; FR; IT)

ANNEX 1

MODEL LETTER FOR REQUESTING ACCESS

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

I_____(name and 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 FOR REQUESTING RECTIFICATION

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

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

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

would like to request rectification of factually inaccurate data relating to me stored in the Schengen Information System. My personal data should be rectified 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 elements justifying the need for rectification.

The Applicant/ The Legal Representative

(Signature)

ANNEX 3

MODEL LETTER FOR REQUESTING ERASURE

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

I_____(name and surname),_____(nationality), _____(date and place of birth), _____(address), would like to request rectification 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 erased 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 elements justifying the need for erasure.

The Applicant/ The Legal Representative

(Signature)