



Council of the  
European Union

**Brussels, 16 December 2014  
(OR. en)**

**16807/14**

**SIRIS 82  
COMIX 668**

**COVER NOTE**

---

From:	Ms Clara Guerra, Chair of the SIS II Supervision Coordination Group
date of receipt:	2 December 2014
To:	Presidency of the Council of the European Union
Subject:	Report on the exercise of the rights of the data subject in the SIS and Guide for exercising the right of access in the SIS

---

Delegations will find attached the report on the exercise of the rights of the data subject in the SIS and the guide for exercising the right of access in the SIS from the SIS II Supervision Coordination Group.

SIS II SUPERVISION COORDINATION GROUP

SECRETARIAT GÉNÉRAL DU  
CONSEIL DE L'UNION EUROPÉENNE  
SGE14/12482  
Reçu le 02-12-2014  
DEST. PRINC. .... M. FERNANDEZ-PITA  
DEST. COPISTES .....

President of the Council of the European Union  
General Secretariat  
Council of the European Union  
Rue de la Loi 175  
B-1048 Brussels

Brussels, 21 November 2014

**Subject: Report on the rights of the data subject and Guide of access adopted by the Schengen Information System (SIS) Supervision Coordination Group**

Dear Mr President,

I have the pleasure of sending you two documents adopted by the SIS II Supervision Coordination Group) during our most recent meeting in Brussels, on 28 October 2014:

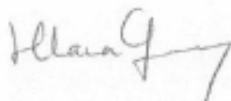
- "Report on the exercise of the rights of the data subject in the Schengen Information System" and
- "The Schengen Information System. A guide for exercising the right of access".

The Report looks into the experience of the Member States of the Schengen Area with responding to requests of individuals when they are exercising their rights of access, correction, deletion and - formerly existing - request for checks. It draws conclusions on the information provided by the competent authorities of the Member States and it makes recommendations to improve harmonisation and reinforce cooperation mechanisms, in order to guarantee the effective exercise by data subjects of their rights stemming from data protection law.

The Guide of Access intends to assist data subjects in the exercise of their rights. It enshrines a description of the procedure for exercising the right of access in each Member State, providing practical information, such as the contact details of the competent authorities, model letters, and formalities for the requests.

In addition, I would like to kindly ask you to support the Group in our tasks of raising awareness by disseminating as widely as possible the useful information contained in the documents enclosed, namely through your websites.

Yours faithfully,



Clara Guerra  
Chair of the SIS II Supervision Coordination Group

Cc: Mr Uwe CORSEPIUS, Secretary-General  
Mr Stefano SANNINO, Permanent Representative of Italy  
Mr Guy STESENS, Secretariat General of the Council

Contact person: Jacob Kornbeck (tel: 02 283 1995)

Enclosed:

- "Report on the exercise of the rights of the data subject in the Schengen Information System";
- "The Schengen Information System. A guide for exercising the right of access".

# **REPORT**

## **on the exercise of the rights of the data subject in the Schengen Information System (SIS)**

**Brussels  
October 2014**

## I. Introduction

1. The “second generation” Schengen Information System (hereinafter, “SIS II”) replaced the Schengen Information System (‘SIS’) on 9 April 2013.
2. Compared to SIS, the SIS II developed new characteristics: widened access to the data processed in SIS II by public authorities (Europol, Eurojust, national prosecutors, vehicle licensing authorities), interlinking of alerts, addition of new categories of data, including biometric data (fingerprints and photographs), as well as a technical platform to be shared with the Visa Information System<sup>1</sup>.
3. The SIS II is at the heart of the Schengen mechanism. It affects the rights of millions of people on a daily basis and contains over 45 million alerts<sup>2</sup>. Data protection is essential for its legitimacy and success in practice.
4. The rights of the data subject are key to data protection, allowing individuals to control the processing of their personal data, within the limits established by law. Ensuring the effectiveness of the rights of the data subject is particularly important in the area of freedom, security and justice, where, on one hand, the exceptions and limitations imposed by law have a larger scope of application, and, on the other hand, the erroneous processing of personal data may have serious direct consequences on the data subject.
5. This report looks into the experience of the Member States of the Schengen area<sup>3</sup> with responding to the requests of the data subjects when they are exercising their rights of access, correction, deletion and - formerly existing - request for checks. The statistics provided by DPAs as an answer to the questionnaire and used as a basis to draft this report mostly relate to SIS II but sometimes relate to the former SIS, in particular on the requests for checks that do not exist anymore in SIS II legislations. Having regard to the challenges that the more complex SIS II can pose to all the actors involved, the purpose of this report is to assess the procedures currently implemented by the supervisory authorities to answer the requests of the data subjects, to find whether there are significant differences in the manner in which they reply and handle these requests and to draw recommendations in order to improve efficiency and consistency in the exercise of the rights of the data subjects with regard to data processing in SIS II.

---

<sup>1</sup> See the Opinion of the European Data Protection Supervisor and the Opinions of the Schengen Joint Supervisory Authority on the SIS II legal package.

<sup>2</sup> According to the most recent available data, “alerts on persons represent 1.71% (861,900 alerts) of the content of SIS II. The biggest category of alert is represented by issued documents (such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated) with 79.23% (39,836,478 alerts) of the total amount of alerts”. See the report issued by EU-LISA in June 2014, “SIS II 2013 - Statistics”, available here: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/20140709\\_sis\\_ii\\_stats\\_2013\\_public\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/20140709_sis_ii_stats_2013_public_en.pdf)

<sup>3</sup> This report is the outcome of an activity that started within the JSA and the SCG of SIS II considered it is an important endeavour and took over the work already done in order to finalize it.

6. After describing the legal background guaranteeing the rights of the data subject in the SIS II<sup>4</sup> (II), the methodology employed (III), the report presents the main findings (IV) and the resulting recommendations (V). The questionnaire is attached as an Annex.

## II. Legal background

7. The SIS II is based on a double legal basis: Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)<sup>5</sup> covers the former first pillar part (hereinafter, “the SIS II Regulation”) while Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)<sup>6</sup> regulates the former third pillar part (hereinafter, “the SIS II Decision”).
8. The classical “right of access, correction of inaccurate data and deletion of unlawfully stored data” is similarly addressed in Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision.
9. In addition, Article 42 of the SIS II Regulation provides for the right of third-country nationals who are the subject of an alert to be informed with regard to the processing of their data, in accordance with Articles 10 and 11 of Directive 95/46/EC. The information shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert. The right is subject to limitations, such as safeguarding national security and the prevention, detection and prosecuting criminal offences, according to Article 42(2). The right to information was not enshrined in the former legal basis of the SIS which was in force when the questionnaire leading to this report was drafted and was therefore not envisaged.
10. The right of persons to have access to data and to obtain the communication of their data “shall be exercised in accordance with the law of the Member State before of which the right is invoked”, according to Article 41(1) of the SIS II Regulation and Article 58(1) of the SIS II Decision. This right is subject to limitations. Accordingly, “information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights freedoms of third parties”<sup>7</sup>.
11. The right of any person to have factually inaccurate data relating to him corrected or unlawfully stored data relating to him deleted is enshrined in Article 41(5) of the SIS II Regulation and Article 58(5) of the SIS II Decision and it is not subject to exceptions.

---

<sup>4</sup> The choice was made not to describe the procedure under SIS even though some of the replies received concerned requests received under the Schengen convention since it is quite similar

<sup>5</sup> OJ L 381, 28.12.2006, p. 4.

<sup>6</sup> OJ L 205, 7.8.2007, p. 63.

<sup>7</sup> Article 41(4) of the SIS II Regulation and Article 58(4) of the SIS II Decision.

12. One of the most important additions brought to the previous legal regime of the SIS is that time limitations are imposed for authorities to reply to the requests of the data subject. The individual shall be informed “as soon as possible, but not later than 60 days from the date on which he applies for access or sooner, if national law so provides”<sup>8</sup>. With respect to correction and deletion requests, authorities shall inform the individual about the follow-up of his request not later than 3 months from the date the request was made<sup>9</sup>.
13. In addition, the data protection provisions from the SIS II Regulation and the SIS II Decision must be interpreted in light of other relevant sources of law<sup>10</sup>.
14. Cooperation between competent authorities of the Member States is also crucial to the effectiveness of the rights of the data subject under the new legal framework. According to Article 41(3) of the SIS II Regulation and Article 58(3) of the SIS II Decision, a Member State other than that which has issued an alert may communicate information concerning personal data processed in the SIS II only if it gives the Member State issuing the alert an opportunity to state its position, a process which shall be done through the exchange of supplementary information.

### III. Methodology

15. 27 national data protection authorities (hereinafter, “DPAs”) have answered the questionnaire: the DPAs from Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden and Switzerland.
16. The data provided by the national DPAs cover two years: 2010 and 2011. Two DPAs have only provided data for 2012 and 2013. However, this fact was taken into account and does not alter the conclusions on the statistics.

---

<sup>8</sup> Article 41(6) of the SIS II Regulation and Article 58(6) of the SIS II Decision.

<sup>9</sup> Article 41(7) of the SIS II Regulation and Article 58(7) of the SIS II Decision.

<sup>10</sup> Article 8 of the European Convention of Human Rights relating to the respect of private and family life; Charter of Fundamental Rights of the European Union's Article 7 on the respect of private life and Article 8 on the respect of personal data protection, Council of Europe Convention no. 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Council Framework Decision 2008/997/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and the free movement of such data; Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 regulating the use of personal data in the police sector.

17. The DPAs which filled in the questionnaire have selectively responded to the proposed questions and sometimes offered raw data in another form than the one asked for, due to practical obstacles. For instance, there were cases in which the competent authorities did not gather separate data on deletion and correction requests, but on both, without differentiating them. These facts were also taken into account and do not alter the findings presented in the Report.

## **IV. Findings**

### **A. General remarks**

18. An evolution of the total number of requests submitted by individuals to exercise their rights with regard to personal data processing in the SIS can be observed from the statistics submitted by the DPAs. More precisely, the number of total requests (access, correction, deletion and checks) increased by approximately 20% from 2010 to 2011<sup>11</sup>. This could be explained by the fact that new Member States have been authorised to use the SIS and that, therefore, the number of data subjects concerned has increased as well.

19. The right the most exercised by data subjects is the right to access personal data, taking into account the available reports of the DPAs which differentiate between the types of requests received by the competent authorities. In the two years covered by the questionnaire, the total number of access requests was 6072, while the total number of deletion requests was 371, the total number of checks – 82 and there was only 1 correction request reported.

20. Most of the requests are made for alerts introduced in the SIS under ex-Article 96 of the Schengen Convention (now Article 24 of SIS II Regulation) – data on aliens for whom an alert has been issued for the purposes of refusing entry<sup>12</sup>.

21. The total number of requests fully granted for 2010 and 2011 is 4161, of which 328 were deletion requests. This represents approximately 63% of the relevant total number of requests made<sup>13</sup>. On the other hand, the total number of requests refused or partly refused is 47. In the same timeframe, 419 requests received a “no data processed” answer.

22. In general, there is not a significant gap between the number of requesters who are nationals in the Member States where the request was made and the number

---

<sup>11</sup> In 2010, there were a total number of 3985 requests reported by the national DPAs, while in 2011 that number was 4795 (the total number does not take into account the statistics provided by the two DPAs which reported data for 2012 and 2013).

<sup>12</sup> 2290 total requests under ex-Article 96 (generally in 2010 and 2011, but taking also into account the report of one DPA for 2012 and 2013).

<sup>13</sup> The Italian DPA did not provide data for the total number of requests which were fully granted, taking into account that it has approximately one third of the total requests received (1045 requests in 2010 and 1209 requests in 2011). Therefore, to obtain an accurate percentage of the requests fully granted, the requests received by the Italian DPA were excluded from the pool of requests.



of requesters who are nationals of another Member States or of a third-country: 941, and, respectively, 891.

23. Additionally, there are DPAs which specifically mentioned in the questionnaire that most of the requests handled by the competent authorities come from citizens residing outside the Schengen area<sup>14</sup>. By contrast, one DPA affirmed that around 90% of the requests are made by residents in the MS of request<sup>15</sup>.
24. Last, it should be taken into account that the SIS II Regulation and the SIS II Decision do not refer anymore to the right of the person to ask the supervisory authorities to check data entered in the SIS, which was previously provided for by Article 114(2) of the Schengen Convention. Nevertheless, the data analysed for this report also contain statistics on requests for checks. The conclusions regarding these requests are mainly presented in Section D, subsection (b). They remain relevant for the SIS II, having regard to the fact that there is a general obligation to cooperate in the new legal framework and the previous experience under check requests could help drawing conclusions on operationalizing the cooperation.

## **B. The role of the DPAs in access requests**

*a) The vast majority of national laws provide for a system of “direct access”*

25. A vast majority of national laws (twenty-one out of twenty-six which answered this question<sup>16</sup>) provide for a system of direct access, according to which the data subject can directly address the data controller with their requests. Five respondents replied that they have a system of indirect access to personal data in the SIS – Belgium, France, Germany, Luxemburg and Portugal, two of which have also a system of direct access – France and Germany<sup>17</sup>.

26. Indirect access is performed through the supervisory authorities, which have the competence to rectify or delete data, if the data were registered in the system by their country.

*b) National DPAs can have an advisory role, a supervisory role and/or the role of an appeal body*

27. The role of the national DPAs in the request for access procedure can take three guises: advisory role<sup>18</sup>, supervisory role and the role of an appeal body. As it was highlighted by one DPA, specific for the indirect access systems is that the DPA

---

<sup>14</sup> The Czech DPA mentioned that “more than 3/4 of requests handled by Police come from citizens from third countries”. The Italian DPA stated that “it should be considered that most of the requests are lodged under art. 96 and that they are lodged by non-EU citizens”.

<sup>15</sup> PT.

<sup>16</sup> BG did not provide answers to this question.

<sup>17</sup> For instance, FR provides indirect access to data processed pursuant to ex-Articles 95, 96, 98 and 99 of the Schengen Convention, and direct access to data processed pursuant to ex-Articles 97 and 100.

<sup>18</sup> In the exercise of its advisory role, PT DPA mentioned the experience of a good practice with NGOs working with immigrants, which guide them to get in touch and go directly to the DPA for exercising their rights with regard to SIS II. The DPA has a Front Office and receives personally data subjects every afternoon and assists them with making requests.

"makes the necessary diligences and then provides the reply to the data subject", thus being "involved in the exercise of the rights' procedures from the very beginning"<sup>19</sup>.

28. There are numerous national DPAs which have the role of an *appeal body* regarding the requests for access<sup>20</sup>.

29. In the relevant period analysed, there were a total of 223 complaints submitted to the DPAs by data subjects who considered their rights were not properly guaranteed by law enforcement authorities<sup>21</sup>.

### **C. Communication of information**

#### *a) Time limits provided by national laws to answer requests vary considerably*

30. The vast majority of national laws provide for a specific time limit to reply to the data subjects when they exercise their rights, with a few exceptions, where the answer must be given "without delay"<sup>22</sup>, "without excessive delay"<sup>23</sup>, "immediately"<sup>24</sup>, or no reference to a time limit is made<sup>25</sup>.

31. The time limits provided for by national laws to answer requests vary considerably, from ten working days<sup>26</sup>, to four months<sup>27</sup>. Most of the national laws provide different time limits for replying to access requests than for replying to correction/deletion requests and checks.

32. In practice, most of the answers are given to data subjects within the maximum limit provided for by law. There are a few cases in which the data subjects receive the replies in less than half of the legal maximum time limit. For instance, four days – in a four weeks' time limit<sup>28</sup>, five days – in a thirty days' time limit<sup>29</sup>, nine days – in a one month time limit<sup>30</sup>.

---

<sup>19</sup> PT.

<sup>20</sup> This is the case of the DPAs from DK, EE, FI, FR (with regard to requests for access under Article 97 and Article 100), GR, LT, MT and SI, which have expressly indicated their role of an appeal body.

<sup>21</sup> Of which 164 from GR, 41 from AT – "all together, not only SIS related", and 19 from MT – between 2009 and 2012, not only in 2010 and 2011. DPAs which received such complaints are from: AT, EE, GR, LI, MT, PL, CH. Some of these DPAs did not expressly mention they're role as an appeal body earlier in the questionnaire. FR and PT specified that this issue is not relevant for the indirect access exercised via their DPAs, where data subjects can directly address the national courts to challenge decisions.

<sup>22</sup> FI – only for correction, deletion and checks.

<sup>23</sup> MT.

<sup>24</sup> DE.

<sup>25</sup> LU.

<sup>26</sup> PT. The DPA specified that, even if the new SIS II legal instruments provide for different (longer) deadlines, it keeps reference of 10 days for access requests and follows the SIS II Regulation and Decision in providing information (not necessarily the final answer) in 90 days.

<sup>27</sup> FR.

<sup>28</sup> DK.

<sup>29</sup> HU.

<sup>30</sup> SE.

*b) No unitary practice with regard to model letters*

33. There is no unitary practice with regard to model letters, even though more DPAs have indicated that they have experience with model letters, than DPAs that do not have such experience. When this is the case, model letters for requests are published either on the webpage of the DPA<sup>31</sup>, or the webpage of the national police service<sup>32</sup>.

*c) Data subjects usually have access to a summary of the content of the alert*

34. There is only one country which mentioned that “nothing is disclosed” to the data subject “with regard to the content of the applicant’s data”, but did not refer to the relevant provisions of national law<sup>33</sup>.

35. Eighteen Member States, out of twenty-four which answered this question, indicated that when communication is granted to the data subject, the communication takes the form of a summary. This could mean, for instance, that “the data subject receives main information regarding the alert, as well as other facts related to the alert, such as who issued the decision which became the legal basis for the alert”<sup>34</sup>. It can also mean that, in addition, the DPA provides for “information related to actions that can be triggered by a data subject in order to obtain the deletion or suspension of the administrative or judicial decision on the basis of which data about him/her are processed in the SIS (for example: request for a non-entry decision to be lifted before the court which pronounced it). Information about judicial remedies is also provided if the data subject has not obtained full or partial disclosure of his/her data when exercising his/her indirect right of access”<sup>35</sup>.

36. None of the countries which have responded to the questionnaire provide a copy of the alert, except for a single case where, instead of the summary of the content, a copy of the alert will be provided “if needed by applicant”<sup>36</sup>.

37. Some of the countries provide, instead of a summary, a list of the processed data<sup>37</sup>, information that the processing in question does not contain any data contrary to the Schengen Convention and the law<sup>38</sup>, (only with regard to ex-Article 96 alerts, now Article 24 of SIS II Regulation) information about the entry

---

<sup>31</sup> FR, PT – for indirect access, GR, LU, NL, ES, CH.

<sup>32</sup> FI, LV, LI, PL, RO, SK, PT. PT DPA mentioned that there are links to the model letters on the webpages of the Ministry of Foreign Affairs, some embassies and consulates websites, as well as in the website of the N-SIS data controller; LI added that the model letter is published both on the websites of the DPA and the police.

<sup>33</sup> LU, which has a system of indirect access: “In case of a request for access the DPA carries out the appropriate verifications and investigations. (...) In case of misuse of the data, the DPA can order the necessary rectification or deletion. The DPA will inform the data subject that the processing in question does not contain any data contrary to the Schengen Convention and the law. Nothing is disclosed with regard to the content of the applicant’s data”.

<sup>34</sup> SK.

<sup>35</sup> FR.

<sup>36</sup> CH.

<sup>37</sup> LI.

<sup>38</sup> LU.

of their personal data into the index of SIS for the purpose of refusal of entry, the period of the alert's validity, the legal basis for the alert<sup>39</sup> and the actual basis for the alert<sup>40</sup>.

d) *Access to the content of the alert is always subject to exceptions and is usually conditioned by the consent of the national competent authorities*

38. Even if access to the content of the alert is provided for in the national law, it is always subject to exceptions, and, usually, to the consent of the national competent authorities<sup>41</sup>.

39. In some of the systems of indirect access, the competent authorities offer access to the content of data to the data subject only after consulting the data controller "following the advice of the police service concerned"<sup>42</sup>, respectively "only with the consent of the data controller"<sup>43</sup>.

40. Exceptions are provided for "essential considerations of private or public interests"<sup>44</sup>, "compromising the purpose of the alert and the police and judicial authorities' action; purpose of the filing system, state security, defence or public security"<sup>45</sup>, "national security; detection of serious crimes"<sup>46</sup>, "jeopardizing the role of the police in preventing, detecting, investigating, and prosecuting criminal offences"<sup>47</sup>, "a judicial or official information blockage, a preponderance of third party interests, internal or external security of the country"<sup>48</sup>. In another case, "the information upon the personal data processed is given in such an extent which does not threaten effectuation of the tasks of the Police Force"<sup>49</sup>.

e) *The majority of countries do not provide reasons of refusal for access requests*

41. Only nine out of twenty-three<sup>50</sup> respondents have expressly indicated that they provide the reasons of refusal to the data subject<sup>51</sup>.

42. There is not a prevalent reason for refusing access among national law, ex-Article 109(2) 1<sup>st</sup> sentence (Article 41(4) of the SIS II Regulation; Article 58(4) of the SIS II Decision) and ex-Article 109(2) 2<sup>nd</sup> sentence (does not have a correspondent

---

<sup>39</sup> NL.

<sup>40</sup> PL and IT - "reasons of the alert".

<sup>41</sup> For instance, DK specifies that according to section 31 of the Danish Data Protection Act, the data subject has the right to access the content of an alert. However, according to section 30 and 32(1), access will not be granted if the interest of the data subject to obtain it is overridden by "essential considerations of private or public interest". Therefore, "in practice, a data subject to an Article 95 and 98-99 alert doesn't get access to the content of an alert according to section 31".

<sup>42</sup> BE.

<sup>43</sup> FR.

<sup>44</sup> DK.

<sup>45</sup> FR.

<sup>46</sup> GR.

<sup>47</sup> MT.

<sup>48</sup> LI.

<sup>49</sup> SK.

<sup>50</sup> 23 of 26 respondents filled in the form to answer to the question regarding reasons for refusal

<sup>51</sup> DK, FI, HU, LV, LI, LU, CH, NL, SE.

in the new legal framework). All the three of them were regularly indicated by the national DPAs in their replies.

43. However, there are some differences with regard to the content of the refusal communicated to the data subject. Some of the DPAs chose an “umbrella” answer for situations in which no data of the requester are processed and situations in which data are processed for the purpose of discreet surveillance, with a view not to jeopardize on-going operations: “there are no data processed subject to the right of access”<sup>52</sup>, “there is no information in the Schengen Information System to be disclosed according to Article 109 CISA”<sup>53</sup>, “the police does not hold any information on him/her that may be given to him/her”<sup>54</sup>, “the DPA has performed the necessary checks”<sup>55</sup>. Very few countries indicated they provide a different answer for refusing access for ex-Article 99 alerts, now Article 36 of SIS II Decision (discreet surveillance and specific checks)<sup>56</sup>, than the answers for ex-Articles 95-98 now respectively Articles 26 and 34 of SIS II Decision.

44. In the case of partial refusals, the content of communication is provided on a case by case basis. For instance, one scenario is to provide only information related to ex-Article 98, now Article 34 of SIS II Decision alerts if the request was made for ex-Article 95 (now Article 26 of SIS II Decision) and ex-Article 98<sup>57</sup>. Another practice is to provide the same information as when the information is fully granted or fully refused, with both versions in the same decision – one for the part which is communicated and one for the part which is refused<sup>58</sup>. Or the data subject can be informed that the authorities do not hold any information concerning them that may be given other than the information provided<sup>59</sup>.

#### **D. Cooperation**

*a) Most of the DPAs will refuse to communicate the data to the requester when the inputting MS has objections against the communication*

45. Most of the responding DPAs have not made any requests of cooperation in 2010 and 2011 (fourteen out of twenty-three which provided answers to this question). Therefore, the total number of requests of cooperation in the relevant period is small - 116, considering that 78 of these were made by one country (FR).

46. Only one DPA confirmed that it used the form for a request of cooperation adopted at the spring conference in Edinburgh on 24 March 2009, but only in

---

<sup>52</sup> AT.

<sup>53</sup> EE.

<sup>54</sup> MT.

<sup>55</sup> PT.

<sup>56</sup> The information given in these cases varies. BE communicates “checks made”, LI gives a “standard answer on carried out check, SK does not give any information (“none”), and NL differentiates between an ex-Article 99 alert for the purpose of specific checks, when “all relevant data will be communicated” and an alert for the purpose of discreet surveillance, when “no data will be given”.

<sup>57</sup> RO.

<sup>58</sup> CH.

<sup>59</sup> MT.

one particular case from 2009 which is currently before the court to decide on<sup>60</sup>. All the others indicated that they do not use it or that they did not have a chance to use it.

47. Few problems were revealed arising from the cooperation procedure. Among these, two can be highlighted: the long period of reply and the use of a language other than English or the national language of the receiving DPA. Other problems mentioned concerned: - cooperation requests sent with incomplete information; requests made through informal, non-verifiable channels; the requested DPA not making a legal assessment of the situation, but simply replicating information provided by the competent authority if its MS in a non-critic way.
48. The few DPAs which provided separate data for the average number of working days in which data subjects receive replies to their requests in cooperation and non-cooperation scenarios have shown that cooperation can prolong the time span of replies. One DPA showed that when the data is inputted in the SIS by the Schengen State in which the request for access is done, the answer is given in four working days, whereas when the data is inputted in the SIS by another Schengen State, the reply is given, on average, in 56,2 days<sup>61</sup>. However, this is a singular case. The other DPAs did not emphasize such big differences of the time span in the two scenarios.
49. With regard to access requests, when the authority receiving the request (LEA or DPA) needs to cooperate with another Schengen State to handle the request, cooperation is almost always foreseen with a law enforcement authority<sup>62</sup>. Most of the national laws provide for cooperation with both law enforcement authorities and national data protection supervisors<sup>63</sup>.
50. Most of the countries will refuse to communicate the data to the requester when the inputting Schengen state has objections against the communication. However, there are a few cases<sup>64</sup> in which national law takes precedence over the negative reply of the inputting state. For instance, the refusal of the inputting state is considered only "one circumstance in the overall assessment of whether access should be granted or not" and in this case, "the final assessment would be based on national law"<sup>65</sup>; or, "an assessment would always be done by the DPA on the reasons put forward for the refusal to communicate data"<sup>66</sup>.
51. One of the noticeable differences between access and deletion/correction requests in the cooperation process is that, with regard to deletion/correction requests where Member States do not reach an agreement, a few Member States mentioned that the matter will be forwarded to the JSA<sup>67</sup>/EDPS for mediation<sup>68</sup>.

---

<sup>60</sup> NL.

<sup>61</sup> DK.

<sup>62</sup> With the exception of LT, where only cooperation with the DPA of inputting Schengen state is foreseen.

<sup>63</sup> Cooperation with the national data protection authority is not foreseen in DK, GR, HU, LI, PL, CH, NL and ES.

<sup>64</sup> FI, LI, SE, PT.

<sup>65</sup> SE.

<sup>66</sup> PT.

<sup>67</sup> now SIS II Supervision Coordination Group

In other cases, a consultation procedure between SIRENE bureaux is initiated<sup>69</sup>, the requester is referred by the law enforcement authority to the national DPA in order to submit a request for deletion by way of mediation<sup>70</sup>, he is referred to the competent authorities of the inputting Schengen State<sup>71</sup>, or the DPA asks for the intervention and assessment of the DPA of the MS concerned and, ultimately, may issue a final binding decision of correction/deletion, only subject to challenge in its national courts<sup>72</sup>.

*b) There is little experience with requests for checks in the cooperation procedure*

52. Most of respondents have signalled that they do not have relevant and significant experience with the cooperation procedure in requests for checks.

53. When the DPA receives a request for check, it exercises its supervisory role and investigates the data controller. For instance, a supervision case was opened against the SIRENE bureau, which was asked to provide the grounds for entering data into the SIS. The grounds were assessed for legal compliance. The conclusion reached in the case was communicated to the requesting authority<sup>73</sup>. In another example, the DPA would check the legitimacy and maintenance of the alert and would advise the requesting DPA accordingly. If the alert appeared not to be lawful, the DPA advised the authority to correct or remove the alert<sup>74</sup>. Another respondent indicated that, in such case, the receiving DPA would contact the national SIRENE Bureau which, if needed, would contact the inputting state's authority and then share the information with the DPA<sup>75</sup>.

54. Some DPAs have more experience with sending requests for checks to other DPAs, than with receiving them. In such instances, the supervisory authorities engaged in a written procedure, in that the supervisory authority of another state was contacted by a letter explaining the details concerning the request for check and the information about the hit in the SIS<sup>76</sup>.

*c) Most of the competent authorities accept requests in other languages than their national language*

55. Almost all the competent authorities accept requests in another language than that of the Schengen State in which the request is done, with only one exception<sup>77</sup>. When receiving a request in another language than their own, the

---

<sup>68</sup> MT, LV

<sup>69</sup> CH.

<sup>70</sup> NL.

<sup>71</sup> ES.

<sup>72</sup> PT.

<sup>73</sup> SE.

<sup>74</sup> NL.

<sup>75</sup> ES.

<sup>76</sup> FI, LT.

<sup>77</sup> Authorities in PL, which also only reply in Polish.

vast majority of the national authorities reply in English, accompanied in some cases by a reply in their language<sup>78</sup>.

56. Cooperation between LEAs and DPAs from the member states is usually done in English. Other languages mentioned more than once in the questionnaire are German, French and Dutch, but they are used in parallel with English.

*d) Third-party mediation is usually sought when the inputting Schengen State comes after the check to a conclusion which is not accepted by the requesting authority*

57. There are very few cases when the supervisory authority of the inputting Schengen State comes to a conclusion that is not accepted by the requesting supervisory authority. Most of the DPAs have answered that such situations never occurred<sup>79</sup>. If such situations should occur, there are several ways which could be used to tackle this issue. For instance, the question will be raised in the plenary meeting of the Joint Supervisory Authority, now the SIS II Supervision Coordination Group, in order to find a common solution<sup>80</sup>, or supplementary clarifications could be asked for before reaching a conclusion<sup>81</sup>, or the data subject will be informed that they could contact the authority of the inputting state directly<sup>82</sup>, or the DPA will contact the other DPA or the JSA to solve the issue by consultation<sup>83</sup>. Only two DPAs mentioned that they will ultimately issue a binding decision, subject to challenge in their national courts<sup>84</sup>.

## V. Recommendations

*a) Recommendations to national competent authorities<sup>85</sup>*

### **- Adopt consistent/harmonised timeframes for answering the requests**

58. The significant variation between the timeframes in which data subjects receive answers to their request indicates that a particular problem raised by the new legal basis of the SIS II is the limitation on the timeframe in which authorities must provide an answer for the requests of access and of correction and deletion. Where the SIS II Regulation applies, it is undisputed that the answer to requests for access should be provided in maximum 60 days, and a follow-up to requests for correction/deletion should be provided in maximum 3 months. However, it is recommended for the authorities to always take into account that the principle is

---

<sup>78</sup> FR primarily replies in French, accompanied by a translation, “when appropriate”. In PT, the DPA deliberation is always in Portuguese, but request for further information may be requested in English or French, besides PT.

<sup>79</sup> DK, FR, GR, HU, LV, LI, LT, MT, RO, SK, SI, SE, CH, PT.

<sup>80</sup> EE.

<sup>81</sup> FR.

<sup>82</sup> LT.

<sup>83</sup> NL and ES.

<sup>84</sup> PT (see para. 51) and AT. In the case of AT, the DPA stated that the “inputting Schengen State has to comply with the binding decision of the DPA”, while “the decision may be subject to a complaint to the High Administrative Court or the High Constitutional Court by the data controller of the SIS data”.

<sup>85</sup> This may also include the DPAs whenever the right to access is exercised indirectly.



to provide a reply “as soon as possible”. Where the SIS II Decision applies, and the national laws do not comply with the “maximum 60 days/maximum 3 months” rules, the authorities should make sure that they provide the replies as soon as possible and in the timeframe provided for by the SIS II Decision, until the national law will be modified according to the provisions of the SIS II Decision.

**- Blanket refusals should always be subject to a prior assessment on a case by case basis**

59. There are cases when a blanket refusal to access data, drafted in general terms, is necessary, especially in the context of on-going investigations. However, it is recommended to always make a prior assessment on a case by case basis, in order to avoid bulk blanket refusals by default. Therefore, the decisions for refusal should be duly substantiated and made available for national DPAs, if requested for the performance of their supervisory tasks.

**- Give the possibility to submit requests in more than one language and, in any case, in English<sup>86</sup>**

60. Taking into account that there is a similar number of requesters from the MS where the request is made and of requesters from outside the MS, it is recommended that the competent authorities accept requests in another language than their national language. They should also be able to reply in another language, so that the exercise of the rights of the data subject will be effective.

**- Improve the cooperation mechanism**

61. It is apparent from the Findings of this report that the field which raises most of the problems related to the exercise of the rights of the data subject in SIS is the cooperation between the competent authorities. In order to improve the cooperation mechanism, the authorities should make sure that they will use in their communication with other authorities a language which is easily comprehended by the agents of the latter.

*b) Recommendations to DPAs*

**- Improve the cooperation mechanism**

62. It is highly recommended that the authorities engaging in cooperation use the form for a request of cooperation adopted at the spring conference in Edinburgh on 24 March 2009.

---

<sup>86</sup> For comprehensive information about how data subjects can exercise the right of access in the SIS II, please consult the updated SIS II Guide for Exercising the Right of Access, which will be uploaded on DPAs websites once finalised.

**- Cooperate with NGOs and other relevant actors in order to raise awareness of the data subjects about their rights**

63. The small number of requests made by data subjects in the exercise of their rights, compared to the number of entries in the SIS II, may have several explanations of which one seems to be the lack of knowledge of data subjects about the existence of their rights and how to exercise them. A solution in this regard could be the cooperation with NGOs working with immigrants or the cooperation with other relevant actors of the civil society in order to raise awareness about the existence and the exercise of the rights of the data subjects in relation to SIS II.

**- Common approach for statistics**

64. Having regard to the difficulties of compiling comparable data from national authorities to efficiently assess various aspects of handling requests made by the data subjects to exercise their rights, there is a need to find a common approach for statistics and their form. To achieve this purpose, one option would be that the Supervision Coordination Group of the SIS II adopts a model form for gathering data, which could be forwarded to the other competent authorities.

ANNEX

**Questionnaire**

**Checklist practice right of access, right of correction and deletion and right to have data checked in Schengen Information System.**

Name Schengen State

Direct Access   
 Indirect Access   
 [If you have both regimes in your MS, please fulfill two questionnaires)

Description of the (possible) role of the national data protection authority in the procedures when a request of access is done.

**A. Statistics**

Requests	REQUESTS							
	Access		Correction		Deletion *		Checks *	
	2010	2011	2010	2011	2010	2011	2010	2011
1.Nr. requests								
a) Nr. positive hits								
i.95								
ii.96								
iii.97								
iv.98								
v.99								
b) Nr. alerts introduced by your MS								

**\*If you have simultaneously a request for access/deletion or a request for checks/deletion, please consider them as deletion request statistical purposes**

Requesters (nr.)	Access		Correction		Deletion		Checks	
	2010	2011	2010	2011	2010	2011	2010	2011

2.1 Residing in MS of request								
2.2 Residing in other Schengen MS								
2.3 Residing outside Schengen								

Results	REQUESTS					
	Access		Correction		Deletion	
	2010	2011	2010	2011	2010	2011
3. Nr. requests fully granted						
i.95						
ii.96						
iii.97						
iv.98						
v.99						
vi. no data processed						
4. Indicate whether national law <b>does not provide</b> for the communication to the data subject of the content of the alert <input type="checkbox"/>	4. a) Indicate if national law <b>does not provide</b> for the communication to the data subject of the content of the correction <input type="checkbox"/>		4. b) Indicate whether national law <b>does not provide</b> for the communication to the data subject of the content of the decision to delete <input type="checkbox"/>			
5. Nr. requests refused or partly refused						
6. Indicate whether national law <b>does not provide</b> for the communication to the data subject of the content of the alert <input type="checkbox"/>	6. a) Indicate whether national law <b>does not provide</b> for the communication to the data subject of the content of the correction <input type="checkbox"/>		6. b) Indicate whether national law <b>does not provide</b> for the communication to the data subject of the content of the decision to delete <input type="checkbox"/>			

7. Nr. of “complaints” submitted to the DPA from individuals who considered their rights of access, correction or deletion were not properly guaranteed by LEA	
--	--

**B. Communication to the data subject**

When granted	REQUESTS			
	Access	Correction	Deletion	Checks
8.1 How is information given to data subject:				
a) in writing				
b) orally				
c) other (specify)				
8.2 What is the content of the communication?				
a)summary				
b)copy of the alert				
c)other (specify)				
<b>When refused</b>				
9. Reason for refusal:				
9.1 article 109(2) first sentence Schengen Convention				
9.2 article 109(2) second sentence Schengen Convention				
9.3 national law				
10. Which information is given to the data subject?				
10.1 access refused				
10.2 referring to reason of refusal				
10.3 other (specify)				
10.4 Is there a different answer when the alert relates to articles 95-98 or to article 99?				
11. If yes, which information is given to the data subject concerning article 99 alerts?				
<b>When partly refused</b>				
12. Which information is given to the data subject?				

### C. Cooperation with other Schengen States

13. When the authority receiving the request (LEA or DPA) needs to cooperate with another Schengen State to handle the request:
- 13.1 **In Access Requests** (article 109 (1) last sentence):
- Is cooperation foreseen with a law enforcement authority ( SIRENE, other)?
  - Is cooperation foreseen with the national data protection supervisor?
  - In which language does this cooperation takes place?
  - When the inputting Schengen State has objections against the communication, does this always lead to a refusal to communicate the data?
- 13.2 **In correction or deletion requests** (article 106 (2)):
- Is cooperation foreseen with a law enforcement authority (SIRENE, other)?
  - Is cooperation foreseen with the national data protection supervisor?
  - In which language does this cooperation takes place?
  - When the inputting Schengen State has objections against the correction/deletion, which further steps are taken?
- 13.3 **In check requests** (article 114 (2)):
- In which language does this cooperation takes place?
  - Please describe the way coordination of the check takes place.
  - What happens when the supervisory authority of the inputting Schengen State comes after the check to a conclusion that is not accepted by the requesting supervisory authority, which further steps are taken?
14. In case of cooperation between two DPA:
- 14.1 Is the form for a request of cooperation used (form adopted at the Spring Conference in Edinburgh on 24 March 2009)? Please mention any experiences with using that form.
- 14.2 How many requests of cooperation did your DPA make (2010; 2011)?
- 14.3 Please mention any problems arising from this cooperation.

#### Time span

- 15.1 Within how many working days, in average, will the data subject get his final answer when the data is inputted in the SIS by the Schengen State in which the request for access is done?
- in access requests:
  - in correction/deletion requests:
  - in check requests:
- 15.2 Within how many working days will the data subject get his final answer when the data is inputted in the SIS by another Schengen State?
- in access requests:
  - in correction/deletion requests:
  - in check requests:
- 16.3 Is there a time limit to reply to the data subject provided by national law or any guidance on this issue? Please give the references.

### **Languages used**

17. Does the competent authority accept requests in another language than of the Schengen State in which the request is done?
18. If yes, which language is used in the communication with the data subject?
  - 18.1 When the request is done in one of the EU languages?
  - 18.2 When the request is done in a non-EU language?

### **D. Miscellaneous**

19. Are there other experiences than mentioned above which are of interest for this survey?
20. Are there experiences with the use of model letters (as developed for the Guide for exercising the right of access).
21. Are the model letters published on the website of the national authorities responsible for SIS and the national data protection authority?
  - 21.1 When the letters are not published, is there a link to the JSA Schengen website in the website of the national authorities responsible for SIS and the national data protection authority?

SIS II SUPERVISION COORDINATION GROUP

**THE SCHENGEN INFORMATION SYSTEM**  
**A GUIDE FOR EXERCISING THE RIGHT OF ACCESS**

---

Secretariat postal address: rue Wiertz 60 - B-1047 Brussels  
Offices: rue Montoyer 30  
E-mail : [EDPS-sis@edps.europa.eu](mailto:EDPS-sis@edps.europa.eu)  
Tel.: 02-283 19 13 - Fax : 02-283 19 50



**This guide has been compiled by  
the SIS II Supervision Coordination Group**

**Address: rue Wiertz 60 - B-1047 Brussels**

**Offices: rue Montoyer 30**

**E-mail : [EDPS-sis@edps.europa.eu](mailto:EDPS-sis@edps.europa.eu)**

**Tel.: 02-283 19 13 -**

**Fax : 02-283 19 50**

## TABLE OF CONTENTS

I.	Introduction to the second generation Schengen information system (SIS II).....	5
II.	Rights recognized to individuals whose data is processed in the SIS II .....	6
II.1.	Right of access.....	7
II.1.1.	Direct access .....	8
II.1.2.	Indirect access.....	8
II.2.	Right to correction and deletion of data .....	9
II.3.	Remedies: the right to complain to the data protection authority or file a judicial proceeding .....	9
III.	Description of the procedure for right of access in each country in the Schengen area....	10
IV.	AUSTRIA.....	11
V.	BELGIUM.....	16
VI.	BULGARIA .....	18
VII.	CZECH REPUBLIC.....	21
VIII.	DENMARK.....	23
IX.	ESTONIA .....	26
X.	FINLAND.....	28
XI.	FRANCE .....	30
XII.	GERMANY .....	33
XIII.	GREECE.....	36
XIV.	HUNGARY .....	39
XV.	ICELAND.....	41
XVI.	ITALY .....	45
XVII.	LATVIA .....	47
XVIII.	LUXEMBOURG.....	49
XIX.	LIECHTENSTEIN .....	51
XX.	LITHUANIA .....	53
XXI.	MALTA.....	57
XXII.	NETHERLANDS .....	59
XXIII.	NORWAY .....	61
XXIV.	POLAND.....	63
XXV.	PORTUGAL.....	67
XXVI.	ROMANIA .....	69
XXVII.	SLOVAK REPUBLIC.....	72

XXVIII. SLOVENIA .....	75
XXIX. SPAIN.....	79
XXX. SWEDEN .....	82
XXXI. SWITZERLAND.....	84
Annexes (Model letters).....	86

Persons whose personal data are collected, held or otherwise processed in the second generation Schengen Information System (hereinafter 'SIS II') are entitled to rights of access, correction of inaccurate data and deletion of unlawfully stored data<sup>1</sup>.

This Guide describes the modalities for exercising those rights.

The Guide falls into three sections: a description of SIS II, of the rights granted to the individuals whose data is processed in SIS II and a description of the procedure for exercising the right of access in each of the countries concerned.

## **I. INTRODUCTION TO THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II)**

The SIS II is a data file shared by all Member States in the Schengen area.

### *Categories of information processed*

It centralises two broad categories of information taking the form of alerts on, firstly, wanted or missing persons, persons under surveillance by the police and persons, not nationals of a Member State of the Schengen area, who are banned from entry into the Schengen territory and, secondly, stolen or missing vehicles and objects such as, in particular, identity papers, vehicle registration certificates and vehicle number plates.

### *Legal basis*

Depending on the type of alert, the SIS II is regulated either by Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System with respect to alert procedures falling under Title IV of the Treaty establishing the European Community (former first pillar)<sup>2</sup> or by Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the

---

<sup>1</sup> These rights are granted under Articles 41 of Regulation (EC) n°1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Article 58 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

<sup>2</sup> Hereinafter 'SIS II Regulation'

second generation Schengen Information System in what concerns procedures falling under Title VI of the Treaty on European Union (former third pillar)<sup>3</sup>.

### *Categories of personal data processed*

When the alert concerns a person, the information can include: (a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; (e) photographs; (f) fingerprints; (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; (k) a reference to the decision giving rise to the alert; (l) action to be taken; (m) link(s) to other alerts issued in SIS II in accordance with Article 37 of the SIS II Regulation<sup>4</sup>.

### *Architecture of the system*

The SIS II is composed of:

- a central system ("Central SIS II");
- a national system (the "N.SIS II") in each Member State (the national data systems that will communicate with the Central SIS II);
- a communication infrastructure between the central system and the national systems providing an encrypted virtual network dedicated to SIS II data and the exchange of data between the authorities responsible for the exchange of all supplementary information \* (SIRENE Bureaux)<sup>5</sup>.

## **II. RIGHTS RECOGNIZED TO INDIVIDUALS WHOSE DATA IS PROCESSED IN THE SIS II**

In accordance with data protection principles, all individuals whose data is processed in the SIS II are recognised specific rights<sup>6</sup> by the aforementioned SIS II decision and regulation.

---

<sup>3</sup> Hereinafter 'SIS II Decision'

<sup>4</sup> See Article 20 of the SIS II Regulation and Decision

<sup>5</sup> SIS II data is entered, updated, deleted and searched via the various national systems. The central system, which performs technical supervision and administration functions, is located in Strasbourg (France). It provides the services for the entry and processing of SIS II data. A backup central system, capable of ensuring all functionalities of the principal central system in the event of failure of this system, is located near Salzburg (Austria). Each Member State is responsible for setting up, operating and maintaining its own national system and for connecting it to the central system. It designates an authority, the national SIS II office (N.SIS II office), which has central responsibility for its national SIS II project. This authority is responsible for the smooth operation and security of its national system.

These are basically:

- the right of access to data relating to them stored in the SIS II;
- the right to correction of inaccurate data or deletion when data have been unlawfully stored;
- the right to bring proceedings before the courts or competent authorities to correct or delete data or to obtain compensation<sup>7</sup>.

Anyone exercising any of these rights can apply to the competent authorities in the Schengen<sup>8</sup> country of his choice. This option is possible because all national databases (N.SIS II) are identical to the central system database (CS.SIS)<sup>9</sup>. Therefore these rights can be exercised in any Schengen country regardless of the State that issue the alert.

When an individual exercises his right of access, correction of inaccurate data and deletion of unlawfully stored data, replies by competent authorities are due within a strict deadline. Thus, without prejudice to shorter national deadlines, the individual shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner, if national law so provides<sup>10</sup>.

Besides, and again without prejudice to shorter national deadlines, the individual shall be informed about the follow-up given to the exercise of his rights of correction and deletion as soon as possible and in any event not later than three months from the date on which he applies for correction or deletion or sooner, if national law so provides<sup>11</sup>.

## II.1. **Right of access**

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

---

<sup>6</sup> See in particular Article 41 of SIS II Regulation and 58 of SIS II Decision

<sup>7</sup> See Article 43 of SIS II Regulation and 59 of SIS II Decision

<sup>8</sup> Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland (situation at May 2014).

<sup>9</sup> See Article 4(1)(b) of SIS II Regulation and Decision.

<sup>10</sup> See Article 41(6) of SIS II Regulation and 58(6) of SIS II Decision.

<sup>11</sup> See Article 41(7) of SIS II Regulation and 58(7) of SIS II Decision

This right is expressly provided for in Article 41 of SIS II Regulation and in article 58 of SIS II Decision.<sup>12</sup>

The right of access must be refused if it could undermine the performance of the legal task specified in the alert, or in order to protect the rights and freedoms of others. It must be refused in any event during the period of validity of an alert for the purpose of discreet surveillance (Article 36 of SIS II Decision).

The right of access is exercised in accordance with the law of the State addressed. The rules of procedure differ from one country to another, as well as the rules for communicating data to the applicant. When a country receives a request for access to an alert which it did not itself issue, that State must give the issuing country the opportunity to state its position as to the possibility of disclosing the data to the applicant<sup>13</sup>.

Also there are currently two types of system governing the right of access to police data files – and thus the SIS. In some countries the right of access is direct, in others it is indirect.

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

#### *II.1.1. Direct access*

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

#### *II.1.2. Indirect access*

---

<sup>12</sup> Both Articles state : 'The right of persons to have access to data relating to them entered in SIS II in accordance with this regulation shall be exercised in accordance with the law of the Member State before which they invoke that right.[...]'

<sup>13</sup> See Articles 41(3) of SIS II Regulation and 58(3) of SIS II Decision

In this case the person sends his request for access to the national data protection authority of the State to which the request is addressed. The data protection authority conducts the necessary verifications to handle the request.

## **II.2. Right to correction and deletion of data**

The right of access is accompanied by the right to obtain the correction of the data relating to them when they are factually inaccurate or incomplete or the right to ask for their deletion when they have been stored unlawfully (Article 41(5) of SIS II Regulation and 58(5) of SIS II Decision).

Under the Schengen legal framework only the State which issues an alert in the SIS may alter or delete it (See Article 34(2) of SIS II Regulation and 49(2) of SIS II Decision).

If the request is submitted in a country that did not issue the alert, the competent authorities of the Member 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 correct or delete the data and gather any relevant information supporting it.

## **II.3. Remedies: the right to complain to the data protection authority or file a judicial proceeding**

Articles 43 of SIS II Regulation and 59 of SIS II Decision present the remedies accessible to individuals when their request has not been satisfied. They recall that any person may bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him.

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



### **III. DESCRIPTION OF THE PROCEDURE FOR RIGHT OF ACCESS IN EACH COUNTRY IN THE SCHENGEN AREA**

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

---

## IV. AUSTRIA

### 1. Nature of right of access

In Austria, the right to information under data protection law is fundamentally direct, i.e. requests for information must be addressed to and answered by the party responsible for processing the data (known as the "*Auftraggeber*" ("controller") in Austria). This rule applies in general under Austrian data protection law and would also apply in particular to information in the SIS II concerning alerts pursuant to Articles 24 of SIS II Regulation and 26, 32, 34, 36 and 38 of SIS II Decision.

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

Requests for information must be addressed to the police authority (as controller) from which the data subject wishes to know if it has processed data concerning him or her. Requests for access from the SIS can be addressed directly to the *Bundeskriminalamt* (Federal Crime Office) which hosts the SIRENE-Bureau. The Austrian Data Protection Authority provides for a form (in German and English) for requests for access to Schengen Data at its website (<http://www.dsb.gv.at/site/6226/default.aspx>).

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

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

- where requested in writing by the data subject (and orally with the controller's consent), and
- if the data subject proves his or her identity in due form (i.e. a copy of an identity card).

The information must include:

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

Information must not be given:

- if necessary to protect the data subject for special reasons,

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

If disclosure has to be refused in order to protect public interests in the field of law enforcement, the remark that "none of the data relating to the data subject which comes under the obligation to provide information has been used" (paragraph 5) must be indicated in all cases in which no information is given (including where no data has actually been used).

Refusals to provide information are subject to verification by the *Datenschutzbehörde* (Data Protection Authority) and to a special appeals procedure.

Information may not be provided if the data subject has failed to cooperate in the course of the information procedure or has failed to pay the legally requested fee.

The data subject must cooperate with reasonable questioning in the course of the information procedure.

Within eight weeks the controller must supply the information or give written reasons for not supplying it in part or in full.

Information is supplied free of charge when it concerns an up-to-date database and when the data subject has not already made the same request in the same year.

In all other cases a flat rate of EUR 18,89 may be charged, which may be varied if higher expenses are actually incurred. If disclosure of the information results in a correction, the fee must be reimbursed.

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

Datenschutzbehörde  
Hohenstaufengasse 3  
A - 1010 Vienna  
Tel.: +43 1 531 15/2525

Fax: +43 1 531 15/2690

E-mail:  
dsb@dsb.gv.at

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

If, in an appeal pursuant to § 31a of the Data Protection Act 2000, the controller pleads the necessity for secrecy in the overriding public interest, the Data Protection Authority must verify whether secrecy was necessary; if not it orders disclosure of the data if secrecy towards the data subject was not warranted.

The authority may, however, appeal to the *Bundesverwaltungsgericht* (Federal Administrative Court). Otherwise the Data Protection Authority's order must be followed within eight weeks, failing which the Data Protection Authority itself may disclose the data to the data subject.

## **5. References of the main national laws that apply**

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

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

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

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

The admissibility of any refusal to provide information on the grounds in Nos 1 to 5 is subject to verification by the Data Protection Authority pursuant to §30(3) and to the special appeals procedure before the Data Protection Authority pursuant to §31(4). (nota bene: it should actually read “pursuant to § 31a”).

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

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

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

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

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

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

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

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

## **6. Language regime**

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

## V. BELGIUM

### 1. Nature of right of access

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

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

Commissie voor de bescherming van de persoonlijke levenssfeer  
Drukpersstraat 35, 1000 Brussel

Commission de la protection de la vie privée  
Rue de la Presse, 35, 1000 Bruxelles

+32 (0)2 274 48 00

+32 (0)2 274 48 35

[commission@privacycommission.be](mailto:commission@privacycommission.be)

Website: <http://www.privacycommission.be>

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

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

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

The procedure is free of charge.

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

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

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

#### **5. References of the main national laws that apply**

- The Act of 8 December 1992 relating to the protection of privacy with regard to the processing of personal data, as amended by the Act of 11 December 1998 transposing Directive 95/46/EC of 24 October 1995, in particular Article 13 thereof;
- The Royal Decree of 13 February 2001 implementing the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data, in particular Articles 36 to 46 thereof.



## **VI. BULGARIA**

### **1. Nature of the right (direct, indirect, mixed)**

Every individual has the right of access to his/her personal data, collected without his/her knowledge and processed in Ministry of Interior's (MoI) information funds or SIS and should submit access request to the national SIRENE Bureau, established as a unit in the International Operative Cooperation Directorate of the MoI.

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

Ministry of Interior of the Republic of Bulgaria

Sofia, 1000

29 "6-th September" str.

Tel.: + 359 2/9825000 – MoI's main office

Web site: <http://www.mvr.bg/contactus.htm>

### **3. Formalities for the request: information and documents to be supplied – possible costs (when the exercise of the rights are free of charge, this should be clearly stated)**

The individuals can exercise their right via the submission of written request (personally or by explicitly authorized individuals with notarial certified letter of attorney) to the personal data controller (in this case- the Minister of Interior).

The request can be submitted also via e-mail under the procedure set in the Electronic Document and Electronic Signature Act.

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.

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

Commission for Personal Data Protection  
Sofia 1592, 2 “Prof. Tsvetan Lazarov” blvd.  
Call centre - Tel.: + 3592/91-53-518

Registry:

Tel.: + 3592/91-53-515, 02/91-53-519

Fax: +3592/91-53-525

E-mail: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

Web site: [www.cdpd.bg](http://www.cdpd.bg)

Every individual has right to request from the CPDP to inspect the data referred to him/her, entered in the Schengen Information System, as well as, to receive information about their usage. If the data are entered by other Member State, CPDP will carry out the inspection in close cooperation with the supervisory authority of this Member State.

- In case that the personal data controller (Minister of Interior) doesn't respect the individual's access request and he/she thinks that there is a violation of LPPD by the processing of his/her personal data (e.g. hindering the exercise of the individual's rights), he/she can submit complaint to CPDP (for starting proceedings under the administrative procedure). If the individual doesn't submit a complaint before the CPDP, he/she could appeal the decision (the refusal of access or submission of information or hindering the exercising of the right of deletion, correction or blocking) before the court. The Commission for Personal Data Protection handles the complaint and adopts decision which after entering into force is binding for the personal data controller. If the complaint's subject was the refusal of access with its decision the CPDP can oblige the controller to exercise the required access and give instructions on the matter.

- When violation by the personal data processing is found, CPDP can impose administrative penalty- fine or property sanction to the personal data controller.

**5. Expected outcome of the requests for access. Content of the information (any specific national deadlines for reply should be inserted here)**

In the Ministry of Interior Act (MIA) is foreseen that every individual has right to request access to his/her personal data, collected without his/her knowledge and processed in the MoI information funds. The personal data controller issues a decision within 14 days from the receipt of the access

request. By expressed wish, to the individual is submitted copy of his/her processed personal data on paper. The bodies of MoI refuse wholly and partially the submission of data:

- when this could endanger the national security or public order; - for protection of information, classified as state or official secret; - when the information sources or implied methods and means for its collection can be disclosed; - if the submission of these individual's data can derogate the exercising of the MoI's tasks determined by law; - or if the information is entered into SIS by another state, which has not allowed its provision. The individuals are notified in writing about the legal ground for the refusal. If the notification is not sent in the legally foreseen deadlines, this is also considered as refusal. Under Art. 161 of the MIA, the refusal is subject to appeal under the procedure set in the Administrative Penal Code.

## **6. References of the main national laws that apply**

- Ministry of Interior Act- prom.SG 17/24.02.2006, last amend. and supplemented SG 70/09.08.2013, in force as from 09.08.2013.

- Regulations on the implementation of the Ministry of Interior Act- adopted with Council of Ministers Decree 126/02.06.2006, prom.SG 47/09.06.2006, last amend. and supplemented SG 10/04.02.2014.

- Ordinance 2727 of 16 November 2010 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria- issued by MoI- in force as from 30.11.2010, last amend. and supplemented SG 28/19.03.2013.

- Ordinance for the amendment and supplement of the Ordinance 2727 of 16 November 2010 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria- issued by MoI- in force as from 19.03.2013, prom. SG 28/19.03.2013.

- Law for Protection of Personal Data- prom.SG 1/04.01.2002, last amend. and suppl. SG 15/15.02.2013.

## **7. Language regime**

The requests for access to data, processed in the Schengen Information System are submitted in Bulgarian.

## **VII. CZECH REPUBLIC**

### **1. Nature of right of access**

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

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

Police Presidium of the Czech Republic  
P. O. Box 62/K-SOU  
Strojnická 27  
170 89 Prague 7

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

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

Any data subject is entitled to send a written request to the Police of the Czech Republic (address given above) asserting his/her right to information on and deletion or correction of his/her data processed in the SIS. Information about the processing of personal data in the SIS is to be revealed only to the data subject concerned (or his/her attorney). The request must contain identification of the applicant – all first name/s, surname, date and place of birth, address, gender and citizenship. In order to ensure unambiguous identification of the applicant and thus reliable processing of request it is recommended to enclose a copy of identification document, which serves as a proof of applicant's identity as well as helps to avoid the risk of disclosure of personal information to unauthorized person. The Police is obliged to answer within 60 days. Exercise of the right of access is free of charge.

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

The Office for Personal Data Protection

Pplk. Sochora 27

170 00 Praha 7

Czech Republic

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

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

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

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

**6. References of the main national laws that apply**

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

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

**7. Language regime**

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

## **VIII. DENMARK**

### **1. Nature of right of access**

The data subject has a right of direct access.

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

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

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

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

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

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

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

Requests for access are free.

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

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

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

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

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

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

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

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

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

## **6. References of the main national laws that apply**

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

## **7. Language regime**

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



## **IX. ESTONIA**

### **1. Nature of the right**

Direct, but in case person asks for access through DPA we do not send him/her to the processor, but we request the information and forward it to person.

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

Police and Border Guard Board

Pärnu mnt 139

15060 TALLINN

telephone 612 3300

fax +372 612 3009

[ppa@politsei.ee](mailto:ppa@politsei.ee)

[www.politsei.ee](http://www.politsei.ee)

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

Application/request signed digitally or on paper, copy of ID card or passport. This exercise is free of charge.

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

Data Protection Inspectorate

Väike-Ameerika 19, 10129

Tallinn, Estonia

[info@aki.ee](mailto:info@aki.ee)

[www.aki.ee](http://www.aki.ee)

DPA have all the rights to supervise alerts and ground documents, demand access, deletion or correction of personal data by percept and institute misdemeanour proceedings. DPA officials have the right to enter, without hindrance, the premises or territory of a processor of personal data for the

purposes of inspection, to access the documents and equipment of a processor of personal data as well as the recorded data and the software used for data processing.

## **5. Expected outcome of the requests for access. Content of the information**

Expected outcome is to grant access as far as it is prescribed by law. In case of protection of any criminal proceedings etc. access is limited to such data. DPA can supervise the validity of such limitation. The national deadline is 30 days.

## **6. References of the main national laws that apply**

[Personal Data Protection Act](#)

[Police and Border Guard Act](#)

[The statutes on the maintenance of the national register of the Schengen information system](#)

## **7. Language regime**

We accept requests in Estonian, English and Russian which are the main languages used. We reply in Estonian and English.

## **X. FINLAND**

### **1. Nature of right of access**

The data subject has a right of direct access.

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

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

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

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

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

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

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

Ratapihantie 9  
PL 800,  
FIN - 00521 Helsinki  
Tel.: ++358 (0)29 56 66700  
Fax: ++358 (0)29 56 66735  
E-mail: [tietosuoja@om.fi](mailto:tietosuoja@om.fi)  
Internet: [www.tietosuoja.fi](http://www.tietosuoja.fi)

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

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

## **5. References of the main national laws that apply**

Data Protection Act (523/1999)

Police Data Protection Act (761/2003)

## **XI. FRANCE**

### **1. Nature of the right of indirect access**

In France, the right of access the Schengen Information System (SIS) is mixed. The right of access is direct for missing persons (*Article 32 of the Council Decision n°2007/533*) or for the persons mentioned or identified in an alert concerning objects (*Article 38 of the same Decision*).

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).

### **2. Contact details of the agency to which the right of access request should be made**

If the request relates to one of the cases where the right of access is direct, it should be made to the :

Direction Centrale de la Police Judiciaire

Ministère de l'intérieur

Place Beauvau

F-75008 Paris

Tél.: +33(0)1.49.27.49.27

Internet: [www.interieur.gouv.fr](http://www.interieur.gouv.fr)

In all other cases, the request should be made to the :

Commission nationale de l'informatique et des libertés

8, rue Vivienne - CS 30223

F-75083 Paris Cedex 02

Tél.: ++33 1 53 73 22 22

Fax: ++33 1 53 73 22 00

E-mail: [mabiven@cnil.fr](mailto:mabiven@cnil.fr)

Internet: [www.cnil.fr](http://www.cnil.fr)

### **3. How to formulate the request : information and requested documents – potential cost**

The right of access is strictly personal. The request for access should be submitted and signed by the applicant (it cannot, under any circumstances, be submitted by a family member or a relative). The applicant can however mandate a lawyer to introduce the request in his or her name, on the condition that the mandate is clearly stated in the request.

There is no particular formal requirement for the request, but the applicant must attach to his letter a legible copy of an official document certifying his or her identity (name, surname, date and place of birth) such as an identity card, a passport, a residence permit, a birth certificate...

The applicant is also welcome to join any other documents that could be useful to carry out the verifications (notification of a visa refusal based on a SIS alert, any favorable decision such as the repealing of an expulsion order).

The right of access proceedings are entirely free.

#### **4. Contact details for the national data protection agency and its role**

Commission nationale de l'informatique et des libertés  
8, rue Vivienne - CS 30223  
F-75083 Paris Cedex 02  
Tél.: ++33 1 53 73 22 22  
Fax: ++33 1 53 73 22 00  
E-mail: [mabiven@cnil.fr](mailto:mabiven@cnil.fr)  
Internet: [www.cnil.fr](http://www.cnil.fr)

Once the request is received, the CNIL appoints one of its members, who is or has been a magistrate of the “Conseil d’Etat”, the “Cour de Cassation” or the “Cour des Comptes”, to carry out the necessary investigations and have the necessary modifications made. In order to do so, the appointed magistrate goes directly to the SIRENE France offices and verifies in person the reason why the applicant is potentially registered in the file.

#### **5. Expected outcome of the requests for access**

After the verifications have been made, the results can only be communicated to the applicant subjected to a national alert if the member of the Commission establishes, with the agreement of the data controller, that the disclosure of the data does not undermine its purposes, State security, the defence or public safety.

When the data controller objects to the disclosure of the information (eg. the person is the subject of discreet or specific checks, the person has an arrest warrant issued against him or her, the person is forbidden from entering the country on grounds of public policy...), the Commission informs the applicant that the necessary verifications have been carried out but that no further information can be given to the applicant (*Article 88 of the Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties*). The Commission also informs the applicant of the means and period of time at his or her disposal in order to contest this objection.

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.

The average processing time varies between one and four months, depending whether or not the applicant is the subject of an alert and whether or not there is a need to undergo further proceedings, such as the cooperation between data protection agencies, in order to verify the validity of the alert.

## **6. References**

Article 41 of the Act No 78-17 of 6 January 1978 modified on Information Technology, Data Files and Civil Liberties.

Article 86 and following of the Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 aforementioned.

## **7. Language regime**

The applicant can submit his or her request either in French or in English.

## **XII. GERMANY**

### **1. Nature of right of access**

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

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

Bundeskriminalamt  
– SIRENE Büro –  
D – 65173 Wiesbaden  
Tel.: ++611 551 65 11  
Fax: ++611 551 65 31

E-mail: [sirenedeu@bka.bund.de](mailto:sirenedeu@bka.bund.de)

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

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

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

If the right of access is exercised through the data protection authority, the requesting citizen is required to provide a signed copy of his or her passport in order to verify his or her identity.

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

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



Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30

D - 53117 Bonn

Tel.: ++49-228-997799-0

Fax: ++49-228-997799-550

E-mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Internet: [www.bfdi.bund.de](http://www.bfdi.bund.de)

If the request concerns an alert pursuant to Article 24 of SIS II Regulation the information is usually disclosed.

If the request concerns an alert pursuant to Article 26 or Article 36 of SIS II Decision, it may be refused if at least one of the generally valid reasons for denying disclosure of information, which are laid down in § 19(4) of the Federal Data Protection Law, is applicable to the request; i.e. if disclosure of the information would jeopardise the proper performance of the tasks incumbent upon the recording body or pose a threat to public security or law and order, or if the data or the fact that they have been recorded must be kept secret by law or by definition, in particular in the overriding interests of a third party, and the interests of the person concerned in obtaining the information must consequently give way.

If the alert was issued by a foreign authority pursuant to Article 26 of SIS II Decision the position of the foreign issuing authority pursuant to the third sentence Article 41(3) of SIS II Regulation or 58(3) of SIS II Decision must be taken into account. The information is usually provided by the *Bundeskriminalamt* – SIRENE Bureau. If the person concerned has applied to the national data protection authority the information is supplied by the Federal Data Protection Commissioner. The information usually includes the legal basis for the alert, the date it was issued and the probable length of time for which it will be kept, as well as the issuing authority.

## **5. References of the main national laws that apply**

The main national texts to be applied are Article 41(3) of SIS II Regulation and 58(3) of SIS II Decision in conjunction with Article 19 of the Federal Data Protection Law or the relevant regulations on the right to information in the laws on data protection at *Länder* level.

## **6. Language regime**

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

### **XIII. GREECE**

#### **1. Nature of right of access**

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

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

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

Ministry of Public Order and Citizen Protection  
Hellenic Police Headquarter  
International Police Cooperation Division  
3d Department - SIRENE  
P. Kanellopoulou 4  
PC: 101 77 Athens  
Tel.: ++301 69 81 957  
Fax: ++301 69 98 264/5  
E-mail: [sirene@police.gr](mailto:sirene@police.gr)  
Internet: ---

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

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

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

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

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

Hellenic Data Protection Authority

Kifisias 1-3, 1st floor

GR – 115 23 Athens

Tel.: ++30 210 6475600

Fax: ++ 301 210 6475628

E-mail: [contact@dpa.gr](mailto:contact@dpa.gr)

Internet: [www.dpa.gr](http://www.dpa.gr)

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

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

If the alert was issued under Article 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 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.

#### **6. References to the main national laws that apply**

The applicable provisions are Article 41 of SIS II Regulation and 58 of SIS II Decision and Article 12 (exercise of the right of access) and Article 13 (exercise of the right to object) of Law 2472/1997.

## **Comment**

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

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

## **XIV. HUNGARY**

### **1. Nature of right of access**

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

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

The SIRENE Office of the National Police Headquarters

H-1139 Budapest, Teve utca 4-6.

Tel: +36 1 443 5861

e-mail: [sirene@nebek.police.hu](mailto:sirene@nebek.police.hu)

Nemzeti Adatvédelmi és Információszabadság Hatóság

Postal address: 1530 Budapest, Pf.: 5.

Office address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Tel: +36 1 391-1400

Fax: +36 1 391-1410

Email: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Web: <http://naih.hu>

In Hungary, 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.

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

The person concerned must provide credible proof of his/her identity and/or his/her authorisation. Requests can be submitted in Hungarian, English, German or French. The information must be given in writing within the shortest possible time, but not later than within 30 days counting from the lodging of the request. The request can be made free of charge. If the data subject repeats within

unreasonable frequency his/her request during a given calendar year, the costs of providing the information will be charged.

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

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 him according to the relevant provisions (52-61.§) of [Act CXII of 2011 on Informational Self-Determination and Freedom of Information \("Privacy Act"\)](#). Furthermore, if the data subject has doubts concerning the answer received from the SIRENE Bureau, or if no answer is received from the SIRENE Bureau, he may apply to the Hungarian National Authority for Data Protection and Freedom of Information.

#### **5. References to 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.

## **XV. ICELAND**

### **1. Nature of right of access**

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 to grant access.

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

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

The CINP's address is:

Ríkislögreglustjórnin  
SIRENE-skrifstofa  
Skúlagata 21  
101 Reykjavík  
ICELAND  
Tel.: ++354 444 2500  
Fax: ++354 444 2501  
E-mail: rls@rls.is  
Internet: www.rls.is

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

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

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



Request must be made by the data subject in person. Proof of identification is required. Information should be given free of charge.

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

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

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

The DPA's address is:

Persónuvernd  
Rauðarárstígur 10  
IS - 105 Reykjavík  
Tel.: ++354 510 9600.  
Fax: ++354 510.9606  
E-mail: [postur@personuvernd.is](mailto:postur@personuvernd.is)  
Internet: [www.personuvernd.is](http://www.personuvernd.is)

If access were not granted, the DPA could give an opinion on the data subject's rights. As of yet, however, the DPA does not have binding powers with regard to SIS II.

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

The Sirene Bureau must answer all applications without undue delay and no later than a month from receipt of the request. If an applicant is registered, he will be informed of the purpose of and reasons

for the registration. In cases where it is necessary to keep the information secret in order to achieve the intended aim of the entry into the information system, or in view of the interests of other persons, or when discreet surveillance is in progress, the data subject does not have the right to be informed of the recorded data. The applicant will be given the same standard reply as an applicant who is not registered, namely "No information is registered/it is not permitted to disclose registered information."

Articles 13 and 15 of the Act on the Schengen Information System in Iceland (<http://www.personuvernd.is/information-in-english/greinar/nr/440>):

#### Article 13

Any person on whom data is entered in the information system (data subject) shall have the right to be informed of the data recorded on him in the system.

The right of a data subject to information under paragraph 1 shall not apply if it is necessary to keep the information secret in order to achieve the intended aim of the entry, or in view of the interests of other persons. When discreet surveillance under Article 7 is in progress, the data subject shall not have the right to be informed of the recorded data.

If a person requests to be informed of data on him that has been entered in the system by another state, that state shall be given an opportunity to express its position before the request is granted.

#### Article 15

When the Commissioner of the Icelandic National Police receives a request under Article 13 or 14, he shall adopt a position on it without unreasonable delay. Reasons for the commissioner's decision shall be given to the extent possible without revealing any information that should be kept secret.

### **6. References of the main national laws that apply**

The main national laws applying are: Act No 16/2000 on the Schengen Information System in Iceland and Regulation No. 110/2000 on the Schengen Information System in Iceland..

### **7. Language regime**

Although not stated in law, Icelandic is the language of administration in Iceland. However, if a request in another language is received by an Icelandic authority, it will be answered. If the request is from an individual who is not in a position to understand an answer in Icelandic (e.g. a foreign

national who does not have an Icelandic party guarding his interests, e.g. a solicitor), he will be answered in a language that he understands.

Information brochures in both English and Icelandic have been printed and issued in the international airport of Keflavik. The data subject is entitled to receive information in a language which he or she understands.

## XVI.

## ITALY

### 1. Nature of right of access

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

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

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

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

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

No special requirements are to be met in order to lodge the application (which may be sent either by post or by fax) nor is there any fee or tax to be paid. The exercise of the right of access is free of charge.

Although there are no express requirements for establishing the applicant's identity in respect of access to the N-SIS in the applicable legislation, in order to expedite the processing of such a complaint, it should be drawn up, if possible, in Italian, English, French or German and **signed by the data subject concerned**, contain a summary description of the grounds on which it is lodged, and be accompanied by a **photocopy of a suitable valid ID pertaining to the data subject**.

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

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

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

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

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

In general an answer (not necessarily a final one) has to be provided within 30 days.

**6. References to the main national laws that apply**

The main national laws applicable are as follows:

- (a) Law No 388 of 30 September 1993, concerning ratification and implementation of the Schengen Agreement and the relevant implementing Convention (see, in particular, Articles 9, 10, 11 and 12);
- (b) Legislative Decree No 196 of 2003.

**7. Language regime**

The application should be drawn up, if possible, in Italian, English, French or German

## **XVII. LATVIA**

### **1. Nature of right of access**

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

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

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

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

#### **State Police**

Čiekurkalna 1.linija 1, k-4

Riga, LV-1026

Ph: +371 67075212; fax +371 67371227

e-mail: [kanc@vp.gov.lv](mailto:kanc@vp.gov.lv)

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

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

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

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

The procedure is free of charge.

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

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

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

#### **5. References of the main national laws that apply**

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

#### **6. Language regime**

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

## **XVIII. LUXEMBOURG**

### **1. Nature of right of access**

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

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

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

Parquet Général du Grand-Duché de Luxembourg  
(Principal State Prosecutor's Office)

BP 15

L-2010 Luxembourg

Tel.: ++352 47 59 81-331

Fax: ++352 47 05 50

E-mail: [parquet.general@mj.etat.lu](mailto:parquet.general@mj.etat.lu)

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

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

The procedure is free of charge.

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

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

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



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

## **5. References to the main national laws that apply**

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

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

## **6. Language regime**

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

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

## **XIX. LIECHTENSTEIN**

### **1. Nature of the right**

The data subject has a right of direct access.

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

Landespolizei des Fürstentums Liechtenstein (National police)

Kommando

Gewerbeweg 4

Postfach 684

9490 Vaduz

FÜRSTENTUM LIECHTENSTEIN

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

The application for access must be addressed to the National Police in writing. The applicant must provide proof of their identity. If the application is not filed in person at the National Police Force, the applicant must provide a certified copy of his/her passport.

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

#### **Data Protection Office**

Kirchstrasse 8

Postfach 684

9490 Vaduz

Liechtenstein

Tel. +423 / 236 60 90

info.dss@llv.li

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

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.

**6. References of the main national laws that apply**

Art. 11 und 12 Data Protection Act;

Art. 34g Act concerning the National Police Force (LGBl. 1989 Nr. 48);

Art. 47-49 Ordinance on the Schengen Information System (SIS) and the SIRENE Office (LGBl. 2011 Nr. 140).

**7. Language regime**

The application should be filed in German.

## **XX. LITHUANIA**

### **1. Nature of right of access**

The data subject has a right of direct access.

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

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

Ministry of the Interior of the Republic of Lithuania  
Šventaragio str. 2, LT-01510 Vilnius  
Lithuania  
Phone +370 5 271 7130, fax +370 5 271 8551  
Email [bendrasisd@vrm.lt](mailto:bendrasisd@vrm.lt)

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

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

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

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

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

data subject's enquiry (Article 25 of the Law on Legal Protection of Personal Data).

Where the data subject, after inspecting his personal data, finds that they are incorrect, incomplete and inaccurate and applies to the data controller, the data controller must check the personal data concerned without delay and at a written request of the data subject submitted in person, by post or by means of electronic communications, rectify the incorrect, incomplete and inaccurate personal data and (or) suspend processing of such personal data, except storage, without delay. If he finds that personal data are being processed unlawfully and unfairly and applies to the data controller, the data controller must check without delay and free of charge the lawfulness and fairness of the processing of personal data and, at a written request of the data subject, destroy the personal data collected unlawfully and unfairly or suspend processing of such personal data, except storage, without delay.

The data controller must inform the data subject and the data recipients of the rectification, destruction of personal data or suspension of processing of personal data at the request of the data subject, without delay (Article 26 of the Law on Legal Protection of Personal Data).

According to paragraph 2 of Article 23 of the Law on Legal Protection of Personal Data the data controller must provide conditions for the data subject to exercise his rights, with the exception of cases provided by law when necessary to ensure:

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

The data subject must be refused information about his personal data where necessary to perform actions regarding the alert or to defend the rights and liberties of third parties. Information concerning personal data must not be disclosed to the data subject within the timeframe valid for alerts on discreet surveillance.

Proper reasons must be given for the data controller's refusal to fulfil the data subject's request. The data controller must inform the data subject of his refusal to provide the requested data within no more than 30 calendar days of receipt of the data subject's request.

Regulations on the Lithuanian National Schengen Information System approved by Order of 17 September 2007 of the Minister of the Interior of the Republic of Lithuania No. 1V-324 provide that in cases where alerts on a data subject have been issued by another Contracting Party, the N.SIS data controller must not disclose information to the data subject concerning personal data on him in the national SIS, until authorization to provide such data has been received from the Contracting Party which issued the alert.

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

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

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

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

request, etc.), where they exist, substantiating the facts mentioned in the data subject's complaint, in order to ensure that the complaint is investigated efficiently.

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

## **6. References of the main national laws that apply**

The Law on Legal Protection of Personal Data

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

## **7. Language regime**

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

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

## **XXI.**

## **MALTA**

### **1. Nature of right of access**

The data subject has a right of direct access.

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

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

Data Protection Officer Insp. Sandro Camilleri

Legal Unit

Police Headquarters

Floriana

Tel: 21224001

Email: [sandro.camilleri@gov.mt](mailto:sandro.camilleri@gov.mt)

### **3. Formalities for the request**

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

### **4. Procedure**

The SIS II Regulation and Decision establish that the right of individuals to request access to their personal data entered in the second generation Schengen Information System (SIS II), is to be exercised in accordance with the domestic law of the competent national authority where the request is submitted.



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

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

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

Office of the Information and Data Protection Commissioner

2, Airways House,

High Street

Sliema.

Malta

Tel: +35623287100, fax: +35623287198

Email: [idpc.info@gov.mt](mailto:idpc.info@gov.mt)

Website: **Error! Hyperlink reference not valid.**

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

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

## **6. References to the applicable national legal framework**

The applicable legal instruments are the Data Protection Act (Cap 440), and regulation S.L. 440.05 applicable to the processing of personal data in the Police sector.

## XXII.

## NETHERLANDS

### 1. Nature of the right of access

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

- a. the proper exercise of policing duties;
- b. the protection of the rights of the person concerned or of the rights and liberties of third parties;
- c. national security.

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

Requests for access to information should be submitted to:

Dutch National Police  
Central Unit, Intelligence division  
Attention of the Data Protection Officer  
PO Box 3016  
NL – 2700 KX Zoetermeer  
Tel.: ++31-79-345 9911  
Fax: ++31-79-345 90 10  
E-mail: mailboxipoljz@klpd.politie.nl

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

On receiving a request for information the Data Protection Officer contacts the person concerned regarding arrangements for dealing with the request. A copy of the identity document must be provided and – where applicable – a copy of the legal authorisation to represent the applicant. A fee of EUR 4.50 may be charged for dealing with requests, but in practice requests are free of charge.

Requests concerning alerts based on the SIS II Regulation will be forwarded to the authority responsible for this category of alerts, the Immigration and Naturalisation Service (Immigratie en Naturalisatiedienst, IND) of the Ministry of Security and Justice.

Requests concerning all other alerts will be dealt with by the competent (police) authorities.

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

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

In case of a dispute regarding the processing of the request an application for mediation may be sent to:

College Bescherming Persoonsgegevens

PO Box 93374

NL – 2509 AJ Den Haag

Tel.: ++31-70-8888500

Fax: ++31-70-8888501

E-mail: <mailto:info@cbpweb.nl>

Internet: [www.cbpweb.nl](http://www.cbpweb.nl)

The application should be submitted within 6 weeks of receipt of the information.

Cases in which a request has been refused will be examined free of charge by the Dutch Data Protection Authority (College Bescherming Persoonsgegevens, CBP). As an alternative, or if mediation by the CBP has failed, an application may be submitted to the District Court (administrative section) to consider the case and decide as it finds appropriate.

#### **5. Language regime**

Requests for access may be written – preferably – in Dutch or English, but will be accepted in French, German or Spanish as well. Applicants using another language should take additional time for translation into account.

## **XXIII. NORWAY**

### **1. Nature of right of access**

The right of access is direct.

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

Kriminalpolitisen  
(National Criminal Investigation Service NCIS)

PO Box 8163 Dep.

NO-0034 OSLO

Tel.: ++47 23 20 80 00

E-mail:

Fax: + +47 23 20 88 80

Internet: [www.kripos.no](http://www.kripos.no)

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

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

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

Datatilsynet

PO Box 8177 Dep.

NO-0034 OSLO

Tel.: +47 22 39 69 00

Fax: + 47 22 42 23 50

E-mail: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no)

Internet: [www.datatilsynet.no](http://www.datatilsynet.no)

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

Applications for access are decided in the first instance by the registration administrator (NSIS). If the application has been made to the registration administrator, it is referred to the authority that

61

ordered the registration with a request for an opinion. If the application has been made to the authority that ordered the registration, this authority forwards it to the registration administrator, accompanied by an opinion.

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

## **6. References of the main national laws that apply**

Act relating to the Schengen Information System (LOV 1999-07-16-66)

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

**1. Nature of right of access**

The right of access to information is direct.

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

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

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

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

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

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

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

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

An application for access is free of charge.

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

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

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

*The request for information should include:*

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

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

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

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

#### *Refusal to provide information on processed personal data*

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

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

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

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

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

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

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

Address for correspondence:

Bureau of the Inspector General for Personal Data Protection (GIODO)  
2 Stawki Street  
00-193 Warsaw  
Poland



tel. +48 (22) 860-73-93

fax +48 (22) 860-70-86

<http://www.giodo.gov.pl>

[kancelaria@giodo.gov.pl](mailto:kancelaria@giodo.gov.pl)

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

## **5. References of the main national laws that apply**

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

## XXV. PORTUGAL

### 1. Nature of the right

The right of access, correction and deletion of personal data processed in the SIS II is exercised indirectly, via the national data protection authority – CNPD.

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

Comissão Nacional de Protecção de Dados – CNPD

Rua de S. Bento, 148, 3º

1200-821 Lisboa

[www.cnpd.pt](http://www.cnpd.pt)

**Front Office - Privacy Line:** (00.351) 393 00 39 (Mondays to Fridays, from 10-13h GMT)

**Personal attendance:** Mondays to Fridays, from 14.30 – 16.30h (GMT)

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

Requests must be submitted in writing, using one of the specific three forms, either for the right of access, the right of correction or the right of deletion. These forms are available on the DPA website in Portuguese, English and French versions. The requests may be submitted in person in the DPA Front Office or sent by post mail. Applicants must present an identification document (passport or ID card for Portuguese citizens). If requests are sent by post mail, it must be enclosed to the form an intelligible and certified copy of the passport or ID card.

Requests are free of charge.

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

Contact details of the CNPD are given in item 2.

All information on the rights of the persons concerning the Schengen Information System is available in PT, EN and FR in the DPA website.

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

The DPA makes all due diligences before the Schengen competent authorities and provide an answer to the requester as soon as possible and, in any case, no longer than 30 days for the access

requests. For the correction and deletion requests, the DPA, if unable to provide a final answer, will inform the requester within 90 days of the follow-up of the request.

## **6. References of the main national laws that apply**

Law 67/98 of 26 October (article 11) – Data Protection Law

## **7. Language regime**

The requests must be submitted in Portuguese, as well as any documents enclosed shall be translated into Portuguese. The Front Office will assist you in fulfilling the request, if necessary.

## XXVI. ROMANIA

### 1. Nature of right of access

The right of access in Romania is direct.

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

According to Article 62 (3) of Law no. 141/2010 on the setting up, organisation and functioning of the National Information System for Alerts (NISA) and participation of Romania to the Schengen Information System, the requests may be submitted to the national SIRENE Bureau or to any data controller within the Minister of Administration and Interior or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

Address for correspondence:  
Centre for International Police Cooperation  
SIRENE Bureau  
1-5 Calea 13 Septembrie, Bucharest, 5<sup>th</sup> District

Romania

Tel.: +40 21 315 96 26

Tel.: +40 21 314 05 40

Fax: +40 21 314 12 66

Fax: +40 21 312 36 00

E-mail: [ccpi@mai.gov.ro](mailto:ccpi@mai.gov.ro)

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

The rights of the person as regards the personal data processing in the NISA or SIS II are used according to the provisions of Law no. 677/2001 on the protection of individuals with regard to the personal data processing and the free movement of such data, with the subsequent modifications and amendments, with the exceptions mentioned by this law.

According to Article 13 (1) of Law no. 677/2001, *an application for access is free of charge.*

The data subject shall not be communicated information regarding personal data processed in NISA or SIS II 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.

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

The legality of the personal data processing in the N.SIS on the territory of Romania and transmitting this data abroad, as well as subsequent exchanging and processing of supplementary information are subject to monitoring and control by the National Supervisory Authority for Personal Data Processing.

The auditing of the personal data processing is performed by the National Supervisory Authority for Personal Data Processing according to audit international standards at least once every four years.

Address for correspondence:

National Supervisory Authority For Personal Data Processing

28-30 G-ral Gheorghe Magheru Bld.

Bucharest, 1<sup>st</sup> district 1

Romania

Tel.: +40 31 805 92 11

Fax: +40 31 805 96 02

E-mail: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro)

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

The requests of the data subjects in the context of personal data processed in the NISA or the SIS II 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, in the case of using the right of access to the personal data and as soon as possible but no later than 90 days after the receipt of the request in the case of using the right of rectification and deletion of the personal data, by exception from the provisions of Law no. 677/2001, with the subsequent modifications and amendments.

## **6. References of the main national laws that apply**

- Law no. 141 of 12<sup>th</sup> of July 2010 on the setting up, organisation and functioning of the National Information System for Alerts (NISA) and participation of Romania to the Schengen Information System,
- Law no. 677 of 21<sup>st</sup> of November 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed.

## **7. Language regime**

If the data subject is Romanian, he/she can submit his/her request in Romanian and if the data subject is foreigner, he/she can submit his/her request in English.

**1. Nature of right of access**

Under Article 41 of SIS II Regulation and 58 of SIS II Decision, anyone has the right to have access to data entered in the second generation Schengen Information System (SIS) which relate to him. This right is to be exercised in accordance with national law of the contracting party. In the case of the Slovak Republic, the data subject has a right of direct access.

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

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

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Pribinova 2, 812 72 Bratislava

Slovenská republika

Phone: 02/5094 1111

Fax: 02/5094 4397

 [send](#) the mail

Internet :<http://www.minv.sk>

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

Under Article 69c of Act No. 171/1993 Coll. on the Police Force everyone has right to request, in writing, that the Ministry of Interior provide information on what personal data is being processed on them. At the same time the controller of the Schengen Information System is obliged to provide the information free of charge within 30 days from the date of receiving such **written request**.

The standard application form for the above request is available on the web site of the Ministry of Interior. The data subject is obliged to provide his/ her personal data (name, surname, permanent address, place and full date of birth and nationality) as well as a copy of his/her ID card or passport for the purpose of proving his/her identity.

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

Provision of personal data to the applicant from the information systems operated by police is executed under Article 69c of the Act No. 171/1993 Coll. on the Police Force.

In the case of the Schengen Information System II, if the alert was issued under Articles 26 - 34 and Article 38 of the SIS II Decision, the applicant will be informed of the data relating to him/ her (at least the following personal data: name, surname, date and place of birth, sex, nationality and reason for the alert i.e. the purpose of the processing of his/her personal data).

Where the right of access to information concerns an alert which was not issued by the Slovak Republic, the issuing country must be given an opportunity to state its position as to the possibility of disclosing the data to the applicant.

If the alert was issued under Article 36 of the SIS II Decision, the applicant is likely to be refused disclosure of the data (the processing has been carried out on national security grounds or in the investigation of particularly serious offences).

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

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

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

Bringing complaints is regulated by the provisions of Section 63 of Act No. 122/2013 Coll. on Personal Data Protection. (The standard form for lodging complaints is available on the website of the Ministry of the Interior too).



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

Úrad na ochranu osobných údajov Slovenskej republiky  
(Office for Personal Data Protection of the Slovak Republic)

Hraničná 12

827 07 Bratislava 27

Slovenská republika

Tel: +421 2 32 31 32 14

Fax: 421 2 32 31 32 34

e-mail:statny.dozor@pdp.gov.sk

Internet:[http:// www.dataprotection.gov.sk](http://www.dataprotection.gov.sk)

**6. References of the main national laws that apply**

Act No. 122/2013 Coll. on Personal Data Protection and on Changing and Amending of other acts,  
as amended by Act No. 84/2014 Coll.

**1. Nature of right of access**

There is a right of direct access.

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

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

Policija, Ministrstvo za notranje zadeve

Štefanova 2

1501 Ljubljana

Slovenia

Fax: + 386 1 428 47 33

E-mail: gp.mnz(at)gov.si

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

Link to the form for Request for Information on Data in the National Schengen Information System in Slovenia (N.SIS), which can be downloaded in English:

<http://www.ip-rs.si/index.php?id=346>

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

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

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

1. enable consultation of the SIS filing system catalogue;

2. certify whether data relating to the data subject are being processed or not, and enable him to consult personal data contained in the national SIS filing system that relate to him, and to transcribe or copy them;
3. supply him with an extract of personal data contained in the national SIS filing system that relate to him;
4. provide a list of data recipients to whom personal data were supplied, stating when, on what basis and for what purpose;
5. provide information on the sources on which records about the individual in the SIS are based, and on the method of processing;
6. provide information on the purpose of processing and the type of personal data being processed in the SIS, and all necessary explanations in this connection;
7. explain the technical and logical-technical procedures of decision-making.

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

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

Informacijski pooblaščenec  
(Information Commissioner)  
Zaloska 59  
1000 Ljubljana  
Slovenia  
Tel.: ++ 386 1 230 97 30  
Fax: ++ 386 1 230 97 78  
E-mail: [gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)  
Internet: [www.ip-rs.si](http://www.ip-rs.si)

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

Applicants who consider that any of their rights have been violated in relation to an application for access may lodge a claim with the Information Commissioner. The Information Commissioner,

having received the complaint, forwards it to the controller of the file, so that he can draw up any statements he regards as relevant. Finally, the Information Commissioner takes a decision on the complaint and forwards it to those concerned, after receiving the statements and the reports, evidence and other investigation documents, as well as inspection of the files where necessary and interviews with the person concerned and the controller of the file.

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

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

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

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

## **6. References of the main national laws that apply**

- Personal Data Protection Act (Official Gazette of the Republic of Slovenia, no. 94/2007, official consolidated text), unofficial English translation of the Act available at: <http://www.ip-rs.si/index.php?id=339>;

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

## **XXIX. SPAIN**

### **1. Nature of right of access**

Data subjects have the right of direct access, but, when the data controller fails to respond to a request for access or when the answer provided is unsatisfactory they also have the right to indirect access through the Spanish Data Protection Authority.

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

Requests for access to information should be submitted to:

Secretaría de Estado de Seguridad  
Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad,  
C/ López Santos, 6,  
28230 Las Rozas (Madrid)  
Spain

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

Any request for access must be submitted in writing to the data controller. To this end, data subjects must send an application to the data controller by any means that provides evidence of the dispatch and receipt of the application.

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

The procedure is free of charge.

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

Agencia Española de Protección de Datos (Data Protection Authority)

C/ Jorge Juan, 6

E - 28001 – Madrid

Tel.: + 34 901 100 099

Fax: + 34 91 445 56 99

E-mail: [ciudadano@agpd.es](mailto:ciudadano@agpd.es)

Internet: [www.agpd.es](http://www.agpd.es)

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

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

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

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

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

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

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

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

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

## **6. Language regime**

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

## **7. Forms**

The Spanish DPA offers through its website an unofficial standard form (in Spanish) for the right of access that can be used at the convenience of the data subject. The form can be found on the following link:

[http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho\\_schengen\\_den/common/DERECHO\\_DE\\_ACCESO\\_Schengen\\_Es.pdf](http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho_schengen_den/common/DERECHO_DE_ACCESO_Schengen_Es.pdf).

Data subjects wishing to lodge a claim related to the right of access with the Spanish Data Protection Authority can use the following link (in Spanish only): <https://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/tipoSolicitud/solicitudPresencial.jsf>



## **XXX. SWEDEN**

### **1. Nature of right of access**

There is a right of direct access.

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

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

Rikspolisstyrelsen  
Box 12256  
Polhemsgatan 30  
S - 102 26 Stockholm  
Tel: ++46 77-114 14 00  
E-mail: rikspolisstyrelsen@polisen.se  
Internet: [www.polisen.se](http://www.polisen.se)

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

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

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

Datainspektionen  
Box 8114  
Drottninggatan 29, 5<sup>th</sup> floor  
S - 104 20 Stockholm  
Tel.: ++46 (0)8-657 61 00  
Fax: ++46 (0)8-652 86 52

E-mail.: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

Internet: [www.datainspektionen.se](http://www.datainspektionen.se)

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

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

Whether or not the information is disclosed depends on the provisions of the Official documents and Secrecy Act (2009:400), which may prohibit the disclosure of certain data. Where disclosure of the data is permitted, the National Police Board is responsible for forwarding it.

#### **6. References to the main national laws that apply**

Law applicable: Sections 26 and 27 of the Personal Data Act (1998:204), Section 8 of the Schengen Information System Act (2000:344) and section 21 of the Schengen Information System regulation (2000:836).

#### **7. Language regime**

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

**1. Nature of right of access**

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

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

Federal Office of Police (fedpol)  
Legal department/ Data protection  
Data Protection adviser  
Nussbaumstrasse 29  
CH-3003 Berne  
[www.fedpol.ch](http://www.fedpol.ch)

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

Individuals' requests concerning their personal data processed in the SIS have to be directly addressed to the Federal Office of Police, controller of the SIS data file in Switzerland. The requests must usually be sent in writing with a copy of a valid identity card or passport and a power of attorney if the person is represented. If a request is sent by email, the person must mention his postal address and annex a copy of a valid identity card or passport.

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

Federal Data Protection and Information Commissioner (FDPIC)  
Feldeggweg 1,  
CH-3003 Berne  
Phone: +41(0)31 322 43 95, Fax +41-(0)31 325 99 96  
<http://www.edoeb.admin.ch/index.html?lang=en>

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

According to Article 50 paragraph 4 of the Ordinance on the National Part of the Schengen Information System (N-SIS) and on the SIRENE Bureau (N-SIS Ordinance), the individual concerned shall be informed within 30 days of receipt of his request for access. If it can't be informed in this time limit, the person must be informed of this delay. The person must be informed not later than 60 days of receipt of the request. If there is no ground for refusal, the individual is fully informed.

According to Article 50 paragraph 5 of the N-SIS Ordinance, the individual concerned shall be informed not later than 3 months from the date on which he applies for his request of correction or deletion.

The right to be informed in case of a decision of non-admission is governed by Article 51 of the N-SIS Ordinance.

## **6. References to the main national laws that apply**

- [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. 235.1)
- [Ordinance on the National Part of the Schengen Information System \(N-SIS\) and on the SIRENE Bureau](#) (N-SIS Ordinance; RS. 362.0)

## **7. Language regime**

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

## Annexes (Model letters)

*The following model letters can be used to file your request unless the national competent authority to which you address your request asks you to use a specific standard form.*

### Annex 1

#### Model letter for requesting access

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

DD-MM-XXXX,

Place

Dear Sir / Madam,

Pursuant to Article 41 of Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System and 58 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System ,

I \_\_\_\_\_ (name, surname), \_\_\_\_\_ (nationality),  
\_\_\_\_\_ (date and place of birth), \_\_\_\_\_ (address), would like to request access to my personal data entered in the Schengen Information System.

Please find enclosed:

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

The Applicant / The Legal Representative

-----

(Signature)

## Annex 2

### Model letter for requesting correction or deletion of the data processed

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

DD-MM-XXXX,

Place

Dear Sir / Madam,

Pursuant to Article 41(5) of Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System or 58 (5) of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System,

I \_\_\_\_\_ (name, \_\_\_\_\_ surname), \_\_\_\_\_ (nationality),  
\_\_\_\_\_ (date and place of birth), \_\_\_\_\_ (address),

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

---

---

---

---

Please find enclosed:

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

The Applicant/The Legal Representative

-----

(Signature)