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[1].

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[2]. 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[3] 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.

[1] See the Opinion of the European Data Protection Supervisor and the Opinions of the Schengen Joint Supervisory Authority on the SIS II legal package.

[2] 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

[3] 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[4] (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)[5] 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)[6] 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"[7].

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.

[4] 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
[5] OJ L 381, 28.12.2006, p. 4.
[6] OJ L 205, 7.8.2007, p. 63.
[7] 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"[8]. 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[9].

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[10].

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.

[8] Article 41(6) of the SIS II Regulation and Article 58(6) of the SIS II Decision.
[9] Article 41(7) of the SIS II Regulation and Article 58(7) of the SIS II Decision.
[10] 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[11]. 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[12].

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[13]. 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

[11] 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).
[12] 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).
[13] 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[14]. By contrast, one DPA affirmed that around 90% of the requests are made by residents in the MS of request[15].

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[16]) 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[17].

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[18], 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

[14] 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".
[15] PT.
[16] BG did not provide answers to this question.
[17] 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.
[18] 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"[19].

28. There are numerous national DPAs which have the role of an *appeal body* regarding the requests for access[20].

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[21].

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"[22], "without excessive delay"[23], "immediately"[24], or no reference to a time limit is made[25].

31. The time limits provided for by national laws to answer requests vary considerably, from ten working days[26], to four months[27]. 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[28], five days – in a thirty days' time limit[29], nine days – in a one month time limit[30].

[19] PT.
[20] 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.
[21] 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.
[22] FI – only for correction, deletion and checks.
[23] MT.
[24] DE.
[25] LU.
[26] 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.
[27] FR.
[28] DK.
[29] HU.
[30] 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[31], or the webpage of the national police service[32].

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[33].

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"[34]. 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"[35].

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"[36].

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

[31] FR, PT – for indirect access, GR, LU, NL, ES, CH.
[32] 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.
[33] 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".*
[34] SK.
[35] FR.
[36] CH.
[37] LI.
[38] 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[39] and the actual basis for the alert[40].

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[41].

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"[42], respectively "only with the consent of the data controller"[43].

40. Exceptions are provided for "essential considerations of private or public interests"[44], "compromising the purpose of the alert and the police and judicial authorities' action; purpose of the filing system, state security, defence or public security"[45], "national security; detection of serious crimes"[46], "jeopardizing the role of the police in preventing, detecting, investigating, and prosecuting criminal offences"[47], "a judicial or official information blockage, a preponderance of third party interests, internal or external security of the country"[48]. 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"[49].

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

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

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

[39] NL.
[40] PL and IT - "reasons of the alert".
[41] 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".
[42] BE.
[43] FR.
[44] DK.
[45] FR.
[46] GR.
[47] MT.
[48] LI.
[49] SK.
[50] 23 of 26 respondents filled in the form to answer to the question regarding reasons for refusal
[51] 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"[52], "there is no information in the Schengen Information System to be disclosed according to Article 109 CISA"[53], "the police does not hold any information on him/her that may be given to him/her"[54], "the DPA has performed the necessary checks"[55]. 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)[56], 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[57]. 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[58]. 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[59].

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

[52] AT.
[53] EE.
[54] MT.
[55] PT.
[56] 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".
[57] RO.
[58] CH.
[59] MT.

one particular case from 2009 which is currently before the court to decide on[60]. 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[61]. 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[62]. Most of the national laws provide for cooperation with both law enforcement authorities and national data protection supervisors[63].

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[64] 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”[65]; or, "an assessment would always be done by the DPA on the reasons put forward for the refusal to communicate data"[66].

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[67]/EDPS for mediation[68].

[60] NL.
[61] DK.
[62] With the exception of LT, where only cooperation with the DPA of inputting Schengen state is foreseen.
[63] Cooperation with the national data protection authority is not foreseen in DK, GR, HU, LI, PL, CH, NL and ES.
[64] FI, LI, SE, PT.
[65] SE.
[66] PT.
[67] now SIS II Supervision Coordination Group

In other cases, a consultation procedure between SIRENE bureaux is initiated[69], 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[70], he is referred to the competent authorities of the inputting Schengen State[71], 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[72].

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[73]. 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[74]. 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[75].

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[76].

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[77]. When receiving a request in another language than their own, the

[68] MT, LV
[69] CH.
[70] NL.
[71] ES.
[72] PT.
[73] SE.
[74] NL.
[75] ES.
[76] FI, LT.
[77] 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[78].

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[79]. 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[80], or supplementary clarifications could be asked for before reaching a conclusion[81], or the data subject will be informed that they could contact the authority of the inputting state directly[82], or the DPA will contact the other DPA or the JSA to solve the issue by consultation[83]. Only two DPAs mentioned that they will ultimately issue a binding decision, subject to challenge in their national courts[84].

V. Recommendations

a) Recommendations to national competent authorities[85]

- 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

[78] 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.
[79] DK, FR, GR, HU, LV, LI, LT, MT, RO, SK, SI, SE, CH, PT.
[80] EE.
[81] FR.
[82] LT.
[83] NL and ES.
[84] 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".
[85] 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[86]

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.

[86] 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 **does not provide** for the communication to the data subject of the content of the alert ☐			4. a) Indicate if national law **does not provide** for the communication to the data subject of the content of the correction ☐		4. b) Indicate whether national law **does not provide** for the communication to the data subject of the content of the decision to delete ☐	
5. Nr. requests refused or partly refused						
6. Indicate whether national law **does not provide** for the communication to the data subject of the content of the alert ☐			6. a) Indicate whether national law **does not provide** for the communication to the data subject of the content of the correction ☐		6. b) Indicate whether national law **does not provide** for the communication to the data subject of the content of the decision to delete ☐	

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)				
When refused				
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?				
When partly refused				
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):
- a) Is cooperation foreseen with a law enforcement authority (SIRENE, other)?
- b) Is cooperation foreseen with the national data protection supervisor?
- c) In which language does this cooperation takes place?
- d) 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)):
- a) Is cooperation foreseen with a law enforcement authority (SIRENE, other)?
- b) Is cooperation foreseen with the national data protection supervisor?
- c) In which language does this cooperation takes place?
- d) When the inputting Schengen State has objections against the correction/deletion, which further steps are taken?

13.3 **In check requests** (article 114 (2)):
- a) In which language does this cooperation takes place?
- b) Please describe the way coordination of the check takes place.
- c) 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.

<u>Time span</u>

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?
- a) in access requests:
- b) in correction/deletion requests:
- c) in check requests:

16.2 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?
- a) in access requests:
- b) in correction/deletion requests:
- c) 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?