VIS SCG

Report on access to the VIS and the exercise of data subjects' rights

February 2016

1. Introduction & Background

The Visa Information System ('VIS') is a system for the exchange of visa data between Member States created by Council Decision 2004/512/EC of 8 June 2004[1] as completed by Regulation (EC) 767/2008 of 9 July 2008[2] ('VIS Regulation') and Council Decision 2008/633/JHA[3]. The system has been operational since October 2011.

As stated in Article 2 of the VIS Regulation, the purpose of the VIS is to facilitate the visa application procedure, prevent visa shopping and fraud, facilitate border checks as well as identity checks within the territory of the Member States and to contribute to the prevention of threats to the internal security of the Member States. To this end, the VIS provides a central repository of data on all short-stay Schengen visas.

These data can be accessed for specific purposes by a number of different actors that are quite often located outside of the EU territory - for instance by authorities issuing visas, e.g. consulates of Member States (Article 15), or by checkpoints at the Schengen border in order to verify the identity of visa holders (Article 18), as well as for the purpose of identifying third-country nationals apprehended within the Schengen Area with fraudulent or without documents (Article 19). Under certain conditions, the VIS may also be accessed for law enforcement purposes.

The present document reports on two important issues from a data protection perspective.

First, given the large number of authorities designated to access the VIS and the different purposes for which they may use the system, access to this system is an issue of great

[1] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.06.2004, p. 5.

[2] Regulation (EC) 2008/767 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13.08.2008, p. 60.

[3] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.08.2008, p. 129-136.

interest to the VIS Supervision Coordination Group ('SCG') as it raises many questions with data protection implications. For instance, which authorities have in fact access to the system? Are some departments allowed wider access than they need to fulfil their tasks? Are the procedures for accessing the VIS compliant with the applicable law?

Second, granting rights to data subjects is an important aspect of data protection. Ensuring that data subjects can effectively access, correct and object to data held about them increases both the transparency of data processing and the data quality for lawful processing, as well as helps to uncover unlawful processing. These considerations are all the more relevant in a field such as visa applications, where compliance with the legal framework is especially important given the adverse consequences that unlawful processing might have.

After describing the legal background setting out the rules to access the VIS and guaranteeing the rights of the data subject in Part 2, and depicting the content of the questionnaires and the applied methodology in Part 3, this report presents the analysis of the answers to those questionnaires in Part 4 and the resulting conclusions and recommendations in Part 5. The questionnaires are attached in the Annexes.

2. Legal background

The data protection framework of the VIS consists of specific rules contained in the legal acts governing this system, namely Regulation (EC) 767/2008 of 9 July 2008 and Council Decision 2008/633/JHA, which complement the provisions of the Charter of Fundamental Rights of the European Union[4], Directive 95/46/EC[5], Regulation (EC) 45/2001[6], Council Framework Decision 2008/977/JHA[7], Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.

With regard to 'normal'[8] access to the VIS, according to Article 6(3) of the VIS Regulation, each Member State shall designate the competent authorities, the duly authorised staff of which shall have access to enter, amend, delete or consult data in the VIS, and communicate a list of those authorities to the European Commission. According to Regulation (EC) 767/2008, different types of authorities can have access to VIS data:

1) Central visa authority/authorities and authority/authorities having central responsibility for issuing visas at the border in the Member State concerned (Articles 15 and 17);

[4] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.
[5] 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, OJ L 281, 23.11.1995, p. 31.
[6] 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 on the free movement of such data, OJ L 8, 12.01.2001, p. 1.
[7] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.
[8] 'Normal' must be understood here as opposed to access to the VIS by law enforcement authorities.

2) Authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code in the Member State concerned (Articles 18 and 20);

3) Authority/authorities having central responsibility for checks within the territory of the Member State concerned (Articles 19 and 20);

4) Authority/authorities having central responsibility for the determination of the Member State responsible for examining an asylum application in accordance with Council Regulation (EC) 343/2003[9] (Articles 21 and 22); and

5) National authority considered as controller in accordance with Article 2(d) of Directive 95/46/EC (Article 41(4)).

On 9 April 2014, the Commission published a consolidated list of Member States' authorities the duly authorised staff of which shall have access to the VIS[10].

With regard to access to the VIS by law enforcement authorities ('LEAs'), according to Article 3 of Council Decision 2008/633/JHA, Member States shall designate the authorities which are authorised to request access to VIS data for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Member States shall notify in a declaration the list of those authorities and of the chosen central access point(s) to the Commission and the General Secretariat of the Council. The Commission shall publish these declarations in the Official Journal of the European Union. Moreover, each Member State shall keep at national level a list of the operating units within the designated authorities that are authorised to request access to the VIS to the central access point(s).

Article 5 of Council Decision 2008/633/JHA sets out the conditions for access by the designated authorities of Member States:

- Access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;
- Access for consultation must be necessary in a specific case; and
- There are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

Finally, with regard to data subjects' rights, Article 37 of the VIS Regulation provides for the right of information and Article 38 for the rights of access, correction and deletion of the data stored in the VIS. Cooperation between Member States to ensure enforcement of the mentioned rights is provided in Article 39. The national supervisory authorities shall, upon request, assist and advise the data subjects in exercising their rights and shall remain available throughout possible proceedings against a Member State refusing access to, correction of or deletion of data (Articles 39 and 40). The liability for damages as a result of an unlawful data processing is subject to national law (Article 33).

[9] Council Regulation (EC) 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ L 50, 25.02.2003, p. 1.

[10] List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS) , OJ C 106, 09.04.2014, p. 4

3. Content of the questionnaires & Methodology

Three questionnaires were adopted following the Group's meeting of 7 May 2014 and subsequently sent to all Member States[11].

The first questionnaire on 'normal' access to VIS data aimed at exploring which authorities have access to VIS data and how this access is actually carried out.

The second questionnaire had the same purposes as the first one, but focused on access to VIS data by LEAs. To this end, the questionnaire was divided into two sections depending on the addressee of the questions, either national access points or data protection authorities ('DPAs').

The third questionnaire on data subjects' rights aimed at investigating how the rights of data subjects are implemented in practice. To this end, it was divided into several sections, some of which were addressed to national competent authorities and one that was addressed to DPAs.

The full questionnaires are respectively reproduced in Annexes I, II and III.

The choice of how to gather the information needed for the purposes of the coordinated inspection was left to the Members of the Group; both desk work and on-the-spot inspections were considered viable options.

4. Analysis of answers

Answers to the three questionnaires were collected throughout the end of 2014 and early 2015. This report is based on answers to the three questionnaires from twenty-two countries[12].

Bulgaria, Croatia, Cyprus and Romania are not yet part of the Schengen Area but nonetheless have a visa policy based on the Schengen acquis. Therefore, these four countries are not connected to the VIS and do not have access to it; such access will be possible once they become Schengen States. In the meantime, they have started preparing for a future connection to the VIS and are taking the necessary technical measures for this purpose. Bulgaria and Romania informed that they have already fulfilled their legal obligations concerning the VIS, as well as their technical obligations relating to the establishment and operation of a national VIS system. They are therefore ready to access the VIS once becoming Schengen States. Cyprus informed that it has not either fulfilled its obligations in this regard.

France could not contribute to the present Report; in this regard, the French DPA regrets the lack of cooperation of the French competent ministry.

[11] When referred to 'Member States' in this report, it must be understood as all countries having access to the VIS.

[12] Answers were provided by Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovenia, Slovakia, Spain and Switzerland.

The number of respondents does not represent the entirety of the 26 countries having access to the VIS[13] but it is still a sufficient number to draw conclusions from the answers that were received.

4.1. First questionnaire on access to VIS data

Q1. Regarding the national authorities included in the consolidated list of competent authorities having access to the VIS published by the Commission, most Member States (19) reported that the consolidated list is currently complete and that no other national authority than the ones already listed has access to the VIS. Three of these Member States pointed out that the consolidated list should clarify that Member States' diplomatic and consular posts in regions where the VIS has been rolled out also consult the VIS, and are in fact the primary users of the VIS when examining visa applications in accordance with Articles 15 of the VIS Regulation. One Member State pointed out that the consolidated list would be more accurate if the relevant police authorities engaged in border controls were specifically identified within the list. One Member State signalled that its list is incomplete and must be rectified. Another Member State sent an updated list of national authorities having access to the VIS in June 2014, which is not yet visible in the consolidated list published by the Commission.

Q2. Twenty Member States confirmed unambiguously that the authorities already included in the consolidated list are indeed competent to have access to VIS data and effectively exercise their access in accordance with the VIS Regulation. Only one Member State signalled that several authorities included in that list do not yet effectively have access to the VIS.

Q3. To the question whether authorities having legitimate access to the VIS data directly or indirectly share the VIS data with other national or international authorities, a majority of Member States (19) answered that as a rule VIS data are not shared with other national or international authorities. Three Member States clarified that this information came from their national authorities and that their DPA had not or could not thoroughly investigate this issue. Several Member States added that VIS data can be communicated to a third country or to an international organisation in exceptional circumstances, for the purpose of proving the identity of third-country nationals, for instance, for the purpose of return, and provided that all requirements of Article 31(2) of the VIS Regulation are met. One Member State specified that, to date, such transfers of data had never occurred. In addition, two Member States mentioned that such transfers can be allowed for other purposes (e.g. when a presumption exists that the visa holder will not comply with the conditions of his/her visa) provided that a legal basis in that sense exists in national law.

Q4. To the question whether internal policies and plans exist within the institutions with a view to ensure that VIS data are used appropriately internally, twelve Member States reported having internal data protection rules and procedures in place to regulate the access and use of VIS data while three Member States indicated that this was not the case. In general, logs of all access are saved and access rights are only granted to a few staff members following a permission procedure. Another Member State reported that access to

[13] The VIS is currently used by 26 countries of the Schengen area, including all four European Free Trade Association (EFTA) member states - Iceland, Liechtenstein, Norway, and Switzerland. Ireland and the United Kingdom do not take part in the VIS.

the VIS outside of EU territory from consular posts is routed through a dedicated network with tunnel encryption. Fourteen Member States confirmed that a general security and data protection policy that also encompasses VIS purposes exists, while one Member State denied this. One Member State announced that such rules are being prepared. Several Members reported that training sessions were organised for users, either beforehand as a requirement to be granted access and/or on a regular basis, sometimes with the involvement of the national DPA. Furthermore, two Member States informed that institutions having access to the VIS are obliged to appoint a Data Protection Officer ('DPO').

Q5. All Member States but one confirmed that their national DPAs had never received complaints about the competence of the institutions. Indeed one Member State received two complaints from data subjects who had requested the deletion of their data in the VIS.

4.2. Second questionnaire on access of law enforcement authorities to VIS data

Q1. Regarding the national authorities authorised to access VIS data for law enforcement purposes, most Member States (18) reported that the list of those authorities notified in a declaration to the Commission is currently complete and that no other LEAs than the ones already listed have access to the VIS. One Member State signalled that to date the administrative procedure to be granted access to the VIS for law enforcement purposes had not been established and therefore the central access point had never been used for such purposes. Another Member State pointed out that two of the authorities mentioned in its declaration have no effective access to the VIS since they have not applied for it. Another signalled that no declaration had been published for its country although national LEAs could access the VIS. Finally, one Member State reported that LEAs do not have access to the VIS and therefore did not provide answers to the second questionnaire.

Q2. Some Member States provided a complete list as referred to in Article 3(5) of Council Decision 2008/633/JHA that is showing the operational units within the designated authorities authorized to access the VIS via the central access point(s). One Member State provided an incomplete list of operational units, as not all designated national authorities did communicate to the DPA which units have access. Finally, two Member States replied that they have the list in question but did not provide it in their answer. One Member State emphasized that access to the VIS was restricted to the relevant operational units within one designated authority on a need-to-know basis. Finally, one Member State signalled that its DPA does not have the list of operational units within the designated national authorities authorized to access VIS data.

Q3. To the question whether designated authorities having access to VIS data directly or indirectly share the VIS data with other national or international authorities, a majority of the Member States (15) answered that as a rule VIS data are not shared with other national or international authorities. Four Member States added that in theory transfers of VIS data by competent LEAs were allowed in exceptional cases as defined in the VIS Decision, although one of them specified that in practice such transfer of data had never occurred. In addition, three Member States answered that national LEAs could also share VIS data with other authorities to the extent necessary for fulfilling their obligations under national law, e.g. to comply with a court order. One Member State signalled that since the administrative

procedure to be granted access for law enforcement purposes is not yet in place, such transfers had never occurred.

Q4. To the question whether internal policies and plans exist within the institutions with a view to ensure that VIS data are used appropriately internally, twelve Member States reported having internal data protection rules and procedures in place to regulate the access and use of VIS data, while three Member States stated that this was not the case. In general, logs of all access are saved and access rights are only granted upon prior authorization to a limited number of staff members. Two Member States further specified that a very detailed written application was necessary to have access to the VIS for law enforcement purposes, with the exception that this application could also be submitted verbally in urgent exceptional cases with an ex-post control. Ten Member States confirmed that a general security and data protection policy that also encompasses VIS law enforcement purposes exists and one Member State replied that such rules are being prepared. In addition, two Member States reported that training sessions were organised for users. Two Member States also indicated that authorities having access to the VIS for law enforcement purposes have a DPO appointed. One Member State reported that none of those policies exist since access for law enforcement purposes is not yet operational.

Q5. Nineteen Member States confirmed that their national DPAs had never received complaints about law enforcement access to the VIS.

Q6. Article 2(1)(e) of Council Decision 2008/633/JHA defines the expression 'designated authorities' as authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. When asked if they considered that based on their national law the designated authorities meet the criteria of Article 2(1)(e), sixteen Member States answered positively. One Member State expressed some doubts regarding one specific designated authority, as at a first glance its main missions do not include the prevention, detection or investigation of terrorist offences or of other serious criminal offences. According to Article 3(6) of Council Decision 2008/633/JHA, only duly empowered staff of the operational units as well as the central access point(s) shall be authorised to access the VIS when all the conditions are met. When asked if they considered that access is restricted to the operational units that need to use it in accordance with Article 3(6), sixteen Member States answered positively, while one Member State said that this was not the case. One Member State added that other operational units than the ones listed in their Declaration should also be granted access to the VIS for law enforcement purposes. Finally, one Member State could not answer this question as its DPA does not have the list of operational units.

4.3. Third questionnaire on data subjects' rights

Q1. Sixteen Member States rated the level of awareness among the relevant staff as regards the obligation to safeguard data subject rights as adequate, satisfactory or even very satisfactory. A "very good" or even "high" rating was given in five other replies. Seven Member States mentioned that relevant staff members who collect and process personal data of visa applicants follow a training course that covers data subjects' rights. One Member State further specified that the Ministry of Foreign Affairs is drafting a new set of

instructions addressed to consular and diplomatic posts, in which due attention is paid to data protection aspects and in particular the exercise of the right of access.

In case of cooperation with external service providers ('ESPs'), Member States were asked how they ensure respect of data subject rights by these subcontractors. Member States referred to Article 43 of the Visa Code and Annex X to the same code[14], which sets out a list of the minimum requirements to be included in contracts concluded with ESPs. Accordingly, twelve Member States reported that contracts signed with ESPs include specific provisions on data protection binding subcontractors, notably in order to ensure respect of data subjects' rights; for instance a clause that explicitly allows the national DPA to conduct on the spot inspections without prior notice, a clause according to which specific information must be made available to visa applicants or a clause that obliges the ESP in question to appoint a DPO entrusted with overseeing respect of data subjects' rights. One respondent said it had "no direct link with subcontractors", whereas two others reported that they do not cooperate with ESPs in this context. In addition, two Member States answered that currently there is no connection with the VIS in places where diplomatic and consular posts cooperate with ESPs.

As to whether DPAs perform quality control regarding the information given to data subjects by subcontractors, one Member State informed that such a control had never been performed. One Member State reported that its Ministry of Foreign Affairs had developed a policy framework for the monitoring of the activities of ESPs, which included monitoring the relevancy of information appearing in leaflets and on ESPs' websites. Similarly, one Member State mentioned that a *vademecum* addressed to offices abroad was available with information on purposes, arrangements, procedural steps and benefits (as well as constraints) in order to ensure the successful outsourcing of the visa issuance process. A few Member States confirmed that their DPA routinely inspects the work of ESPs, while another one reported that diplomatic missions and consular posts are called upon to check that ESPs abide by the clauses laid down in their contracts and to carry out checks on the quality and content of the information made available to data subjects.

Q2. Article 14 of Council Decision 2008/633/JHA concerning the rights of access, correction and deletion makes the exercise of data subjects' rights subject to the provisions laid down in national legislation. Member States were asked whether their national rules would provide for data subjects rights to be exercised directly (through the data controller) or indirectly (through the DPA). Ten Member States pointed to direct exercise, six to a combination of direct and indirect exercise and two to indirect exercise of data subjects' rights. As to what relevant national legal provisions apply, fourteen Member States replied that the national data protection act constituted the legal basis for the exercise of data subjects' rights, while three other respondents identified a national VIS ordinance or regulation. Two Member States referred to a national act governing data processing by police forces.

Q3. When asked how data subjects are informed of the processing and collection of data concerning them, twenty Member States affirmed that this information is provided within the harmonised visa application form. This form also informs data subjects that they have the right to have any data retained about them rectified when data are inaccurate, or

[14] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), Annex X, OJ L 243, 15.09.2009, pp. 47-48.

erased when data were processed unlawfully. Member States provided several examples of this form in different languages.

In addition, eleven replies pointed to additional information channels, including websites of DPAs, diplomatic missions and consular posts, leaflets and factsheets made available at front desks or in waiting rooms of diplomatic missions, consular posts and ESPs, and information provided orally by consular staff. Two Member States reported that information sheets that cover *inter alia* the exercise of data subjects' rights were provided by the Commission and were to be displayed inside diplomatic missions and consular posts, as well as outside for information after working hours.

As to national laws complementing the VIS Regulation, twelve replies referred to the national data protection act, one to a public administration act, one to a freedom of information act and three to a national VIS act.

Q4. As to the usefulness of the abovementioned means employed to inform data subjects about their rights (e.g. such as the leaflets regarding the VIS), thirteen Member States regarded these means as adequate or good. Five Member States answered that they had not enough information to assess this question. One reply also suggested that more could be done in terms of information of data subjects, for example by putting posters in public spaces. In addition, one Member State reported that diplomatic missions and consular posts sometimes fail to disseminate adequately the above mentioned information sheet on data subjects' rights made available by the Commission.

Q5. When asked if they had received any complaints about the information provided in accordance with the Article 37(2) and (3)[15] of the VIS Regulation regarding the right of information, nineteen Member States reported a total absence of complaints.

Q6. In cases in which visas are issued on behalf of another Member State, seventeen Member States reported that they do not insert different information into the visa application forms. In fact, the information in visa application forms used is the same in all Member States. Three Member States specified that the only difference is the appealing procedure in cases of decisions of refusal, annulment or revocation of visas; in this regard data subjects will obtain the relevant (and therefore different) information on the domestic law of the Member State concerned in writing. Two Member States explained that they never issued visas for other countries, in one case on account of not being a Schengen Member.

Q7. Member States were asked to describe the procedures in force for granting the right of access (e.g. formal requirements, time limits for replying, fees, possible exemptions). They were further asked how the right of access is exercised in accordance with Article 14 of the VIS Council Decision 2008/633/JHA, and were invited to provide relevant excerpts of national provisions that do apply and statistics, if available. Detailed descriptions of national procedures, often with excerpts from national legislation translated into English, were

[15] Article 37(2) and (3) states that *"The information referred to in paragraph 1 shall be provided in writing to the applicant when the data from the application form, the photograph and the fingerprint data as referred to in Article 9(4), (5) and (6) are collected"* and that *"The information referred to in paragraph 1 shall be provided to the persons referred to in Article 9(4)(f) on the forms to be signed by those persons providing proof of invitation, sponsorship and accommodation"*.

provided in fifteen cases. The procedures are generally close to the prescription made at EU level.

With regard to possible fees, six Member States reported that the procedures are free of charge. Three others reported that the procedures are free of charge as long as there is not more than one request per year in two of them, or two requests per year in the third one; one of them also specified that in case a fee is charged it may not exceed the immediate costs of providing access and another stated that any fee has to be reimbursed if the processing in question was found to be unlawful or if any information was rectified.

With regard to time limits for replying, three Member States answered that the reply shall be immediate or without delay. Two Member States reported that an answer has to be given within a reasonable interval. Five Member States answered that their procedure provided for a time limit of 30 days.

Two Member States mentioned exemptions to the right of access in their answer to the questionnaire. These exemptions are based on different grounds such as national security, other safety aspects or the protection of the rights of other persons.

Finally, Member States were asked how many requests they had recorded in accordance with Article 38(1) of the VIS Regulation. Nine Member States reported no request at all. In one case, thirteen access requests were reported and in another one 147 requests. This last Member state specified that is not possible to differentiate between requests based on the VIS Regulation and requests based on national legislation. One last Member State reported figures with a specific distinction between requests based on the VIS Regulation (1 request) and Council Decision 2008/633/JHA (2 requests).

Q8. The Member States were asked to describe the general procedures in force for granting the right to correction in accordance with Article 38(2) of the VIS Regulation and to provide statistics, if available. There were only statistics in one case, counting one single request in 2013 and another one in 2014. Three Member States indicated that they do not have any statistics concerning this issue and eight Member States replied that they simply had never received requests for the correction of personal data in the VIS so far. As to the description of the procedures, four Member States stated that the procedures regarding correction are similar to the procedures for granting the right of access already described in their reply to Question 7. Eight Member States confirmed that their national law would provide for a procedure to ensure the respect of the right to correction and eight Member States described the procedure they had set up in accordance with Article 38(2).

Q9. Member States were asked to explain how Article 5 of Council Decision 2008/633/JHA regarding the conditions for access to VIS data by designated authorities of Member States is applied at national level, and to provide details of specific provisions in national law, as well as statistics, if available. The operating units within the designated national authorities may access VIS data only through a central access point designated in each Member State. One Member State reported that instructions for its designated authority to carry out this procedure were available internally. One Member State reported that designated LEAs have to select in advance the purpose for which they seek access to VIS data from an exhaustive list.

Several Member States referred to a national act where all the conditions for LEAs to request access to the VIS laid down in Article 5 of Council Decision 2008/633/JHA are fully

transposed, as well as the fact that the VIS data that may be used for these searches are limited[16].

One Member State provided the number of requests for access to VIS data made pursuant to Article 5 by two designated authorities, i.e. 34 from the police and 10 from the public prosecutor's office from September 2013 to September 2014.

Three replies emphasised that the national competent authorities never received such a request. Three Member States explained that these rules are not currently being enforced at national level and that access to the VIS is only possible in the context of the visa application process.

Q.10 Regarding the procedures in force for granting the right to deletion in accordance with Article 38(2) and (4) of VIS Regulation and Article 14(5) of VIS Council Decision 2008/633/JHA, most Member States confirmed that such procedures exist. Eight Member States gave a description of the procedure, showing that it is in accordance with Article 38(2) and (4) of the VIS Regulation and Article 14(5) of Council Decision 2008/633/JHA. Seven Member States specified that the procedures in question would be provided for by national data protection law, and in one Member State the procedures would be provided for by national administrative law. One Member State reported that there was no authorization for the deletion of personal data granted to the Ministry of Foreign Affairs.

In answering this question, four Member States referred to their answer in Question 7 concerning the procedures for granting the right of access and stated that the procedures are similar. Six Member States made the same statement concerning their answer in Question 8 regarding the procedures for granting the right to correction.

Eight Member States specified that they had never received any request for deletion; four Member States reported that they have no statistics concerning deletions and one Member State did provide statistics, showing a total of two requests in accordance with Article 14 of VIS Council Decision 2008/633/JHA as of September 2014.

Finally, a few Members States provided information on the delay applied to answer requests for deletion of data, which goes from 30 days to 60 days in practice.

Q11. When asked how the competent authorities cooperate actively to enforce the rights laid down in Article 38(2), (3) and (4), three Member States pointed to the use of the VIS-Mail system as a secure communication channel. Four Member States referred to national law regulating the cooperation in accordance with Article 38, including a time limit of 14 days to contact the Member State that recorded the data in the VIS. Two Member States reported that requests concerning another Member State are forwarded rapidly to that competent Member State. Four Member States indicated that there were no requests yet, but that they would cooperate in the case of a request. One Member State specified that it would verify the exactitude of an incoming request from a competent authority before proceeding as foreseen in Article 38.

Q.12 When asked how Article 38(6) of the VIS Regulation was applied in practice and what procedure was being followed in case a request for access, information, correction or deletion is denied, seven Member States reported that the reasons for refusing the request

[16] If a search within any of the accessible data is successful, the designated authorities may in addition access other VIS data.

shall be communicated to the data subject and that the data subject shall be informed about the possibilities for seeking a remedy. In such cases, nine Member States answered that the data subject could address his or her national DPA for review of the decision of refusal. One Member State reported that in the case of a negative decision, the data subject could file an appeal to a court. Five Member States answered that data subjects can either address the DPA, a court or both. Two of those Member States made reference to a time limit of 6 weeks in one case and 3 months in the other, within which a court can be addressed after having contacted the DPA. One Member State indicated that the appeals body depends on the case: concerning refusal of access, data subjects can turn to the DPA, concerning refusal of correction or deletion data subjects can address a court. One Member State indicated that the data subject could also turn to the Ministry of Justice for review, in addition to the DPA, which is the final administrative authority to review a decision. One Member State answered that redress is provided through the DPO of the Ministry and eventually through the DPA. Finally, five Member States emphasized that a case of refusal in accordance with Article 38(6) did not yet occur in practice and one of them stated that this might be due to the relatively small number of biometrics-based visas that were issued until late 2014.

Q13. As to whether the deadline of 60 days as required by the Article 14(6) of Council Decision 2008/633/JHA is respected in practice, seven Member States confirmed that the deadline is respected in practice. In two cases, national rules provide for a shorter deadline, while in one case 3 days are reported to be the normal delay in practice. Five Member States stated that they lacked data; in one case because these rules have not been implemented nationally. Seven Member States reportedly never had such a case.

Q14. As to the number of reviews of decisions of refusal and how they were dealt with in practice, fourteen Member States reportedly never had a case, while six had no statistics. One Member State reported one case per year in 2013 and 2014 respectively. Details on how reviews were dealt with in practice were not provided.

Q15. As regards the outcome (granted, partially granted, denied) of requests made in each of these categories, and whether or not exemptions had been used for granting or denying requests respectively, ten Member States responded that they either had not had any cases, or did not have any relevant data. One Member State had access to such statistics, which showed that 97% of requests had been granted, while in the remaining cases access was denied "because the requesting party was found not to be part of the specific visa application".

Q16. Asked how long it would take, on average, to supply the final answer to the data subject or to rectify data, nine Member States informed that they either had not had any cases, or did not have any relevant data. One Member State reported that all requests would be processed within five working days and another within seven working days.

Q17. When asked to assess the situation in general, including the question whether the procedures in force are seen as satisfactory and, if not (or if only partially so), how they could be improved, nine Member States found the procedures satisfactory, and three found them adequate, while four lacked data or found it premature to give a reply at this stage. One Member State reported its DPA has no knowledge of procedures in place for processing possible requests of data subjects.

Q18. The Member States were further asked how knowledgeable they judged competent authorities to be with regards to their obligations related to data subjects' rights. They were asked whether they thought that the level of information provided to visa applicants is sufficient and to provide relevant excerpts. Finally, they were asked to consider the level of information provided regarding the possibility that VIS data could be also accessed for law enforcement purposes and whether they found it appropriate. Fourteen Member States affirmed, with various nuances, that the competent authorities were sufficiently knowledgeable, whereas three answers suggested that there was room for improvement. One respondent suggested that a fact sheet addressed to visa applicants might be helpful, while another would welcome information material that would more specifically include law enforcement access. One Member State noted that applicants seem to possess only the knowledge provided in the harmonised visa application form, that more targeted information would be needed, and that the websites of competent authorities were found to include some inconsistencies. One Member State found the level of information available appropriate concerning the future access to VIS data for law enforcement purposes. Finally, one Member State did not have sufficient information to assess these questions.

Q19. As to the outsourcing of visa-related work and whether contractors had been found to respect data subjects' rights, three Member States answered that ensuring respect of data subjects' rights was an issue specifically covered by contracts concluded with ESPs. One reply also referred to specific contractual clauses allowing the supervision of data processing and collection by ESPs by national DPAs. One Member State explained that the same safeguards apply to ESPs and that outsourcing should be equally secure and safe for data subjects and the processing of their data. In this regard, another Member State reported that the contractual arrangements concluded with ESPs were considered in line with the data protection legislation.

In addition, several Member States stated that data subjects' rights are sufficiently respected according to their DPA. In three Member States, the national DPA conducted inspections at one or several ESP(s), part of which focused on the exercise of data subjects' rights and the procedures in place. In one case, the DPA specifically looked into the quality of the information provided to data subjects by the ESP and did not find violations. In the other, the DPA considered the procedures, notably for the right of access, as adequate despite a few amount of requests. Some replies indicated that the question was difficult to assess.

Two Member States informed that they do not outsource the visa issuance process. Another explained that ESPs do not have access to VIS data. Finally, one Member State stated that this could become a bigger challenge when the VIS is rolled out in countries where ESPs are used.

Q20. With regard to Article 39(2) of the VIS Regulation concerning the cooperation between DPAs to ensure the rights to correction and deletion, Member States were asked the number of requests for cooperation received and whether DPAs have specific procedures in place. Sixteen Member States reported that their DPA had never received requests for cooperation with other DPAs; one of them also emphasized that their DPA had never received requests from data subjects to correct or delete data concerning them. Two Member States referred to a similar cooperation taking place in the context of the Schengen

Information System second generation ('SIS II'); one of them stated that in such a case the same principles as those followed for similar requests in the context of SIS II would apply.

One Member State reported that its national DPA had received 5 to 10 requests for correction or deletion per year from data subjects; in average two of them needed international cooperation. It further explained that requests for cooperation are addressed to other DPAs in English; those are treated as priority and data subjects are kept informed of the process. Another Member State answered that the national DPA had received two requests for deletion so far, which were forwarded to the controllers.

Member States were further asked how they evaluate the level of cooperation with other Member States' authorities and, if applicable, the procedure followed when applying Article 39(3). Member States could not assess the level of cooperation between DPAs as they never went through this procedure; one of them stated that in case such cooperation were to occur its level would certainly be good.

Q21. As regards the Member States' assessment of the situation overall, whether the procedures in force are deemed satisfactory and, if not (or if only partially so), where the Member States see room for improvement, thirteen Member States found the procedures good or satisfactory. Some replies indicated that the DPAs found the question difficult to assess for different reasons. Several Member States invoked the low number (or the total absence) of requests from data subjects to exercise their data protection rights. Another conveyed that the multiplicity of competences of authorities at national level might make it difficult for these to gain awareness of their role regarding the system and of their obligations vis-à-vis data subjects. One Member State suggested that more detailed information could be made available on websites. Another Member State answered that great work remains to be done regarding the procedures to safeguard data subjects' rights.

In addition, Member States saw room for improvement regarding the information given to data subjects and regarding the use of ESPs, as it raises many questions and no standard practices for Member States exist. One reply referred to several inspections at the national access point, diplomatic missions and consular posts that were conducted and as a result of which specific recommendations were issued. For instance, training consulates' officials and conducting regular checks of the access to the national system.

5. Conclusions & Recommendations

The VIS SCG welcomes all in all the progress achieved so far on issues as important as access to the VIS and data subjects' rights and encourages the Member States to go further to ensure compliance with the legal framework of the VIS in every detail. Based on the analysis of the replies to the three questionnaires, the Group has several remarks and recommendations set out below.

With regard to access to VIS data in general, the VIS SCG stresses that authorities having access to the VIS, and in particular authorities that not only consult the VIS but may enter, amend and/or delete data in the system, should be exclusively those identified in the VIS Regulation for the purposes laid down therein.

The VIS SCG recommends updating the consolidated list of competent authorities having access to the VIS published by the Commission, and clarifying in the document that diplomatic missions and consular posts in regions where the VIS has been rolled out have access to the VIS.

The Group further recommends that competent national authorities (including LEAs), which have not yet done so, develop and formally adopt internal policies regarding access to and use of VIS data as well as security and data protection policies encompassing VIS purposes. In this regard, the VIS SCG welcomes the organisation of training sessions for end users and suggests making them a pre-requisite to be granted access rights to the system.

With regard to access by LEAs more specifically, the VIS SCG recommends updating the declarations published in the Official Journal of the EU pursuant to Article 3(4) of the VIS Council Decision, in which Member States notify to the Commission the list of national LEAs authorised to access VIS data and the central access point(s) through which such accesses are done.

It should be noted that direct access by national LEAs and Europol is not provided for by the VIS Council Decision. Therefore, access by LEAS and Europol to VIS data should be carried out solely through central access point(s) in accordance with the conditions and procedures established by the same text.

In addition, Member States might cross-check the list of operational units within their designated national LEAs authorized to access the VIS via the central access point(s), in order to ensure that access is restricted to the operational units that need to use VIS data in accordance with Article 3(6) of Council Decision 2008/633/JHA.

With regard to data subjects' rights, the VIS SCG welcomes the Member States' assessment according to which relevant staff members of their competent authorities dealing with VIS data have a satisfactory level of awareness regarding their obligation to safeguard data subjects' rights. Furthermore, the Group welcomes the fact that training courses covering data subjects' rights are delivered to the relevant staff in some Member States and encourages others to follow the same approach.

On the other hand, the VIS SCG takes note of the global absence, or in a few Member States the very low number of requests, made by data subjects to exercise their rights of access, correction and deletion of their personal data stored in the VIS, knowing that the system first became operational more than four years ago. This trend might be explained by data subjects' unawareness of the very existence of their data protection rights but also by the lack of information about the way to exercise them (e.g. to whom data subjects should address their requests?). There is a great need to raise awareness among visa applicants in this regard, and even more in cases where applications for a visa are rejected.

As a first step, DPAs should ensure that diplomatic missions and consular posts abroad as well as ESPs make the relevant information regarding visa applicants' data protection rights available, e.g. by performing quality controls regarding the information provided to data subjects.

The VIS SCG will further reflect on best practices to increase information provided to visa applicants about their data protection rights and the procedures to follow.

As regards the procedures in place to answer data subjects' requests to access, correct or delete their personal data stored in the system, the Group encourages Member States to better define the expression "without delay" in Article 38 of the VIS Regulation and adopt uniform maximum time limits for replying in writing to such requests.

Furthermore, in cases where data subjects' requests are denied, the VIS SCGs reminds that, pursuant to Article 38(6) of the VIS Regulation, the decision of refusal should be addressed to data subjects in writing and indicate at least the grounds for refusal and information on how to bring an action or a complaint before the national competent authorities or courts of the concerned Member State.

Finally, since only a few Member States were able to provide statistics regarding the exercise of data subjects' rights of access, correction and deletion and the number of cases in which those requests were denied, the VIS SCGC suggests that Member States find a common approach for keeping such statistics, which would also differentiate between the different types of requests submitted.

Brussels, February 2016

Annex I. First questionnaire on access to VIS data

Questions for the DPAs	
Q 1	Are there any other national authorities apart of those already mentioned that should be included in the consolidated list?
Q 2	Are the institutions already included in the list competent to have access to VIS data as required by the VIS Regulation?
Q 3	Do the authorities having legitimate access to the VIS data directly or indirectly share the VIS data with other national or international authorities?
Q 4	Do internal policies and plans exist within the institutions with a view to ensuring that VIS data is used appropriately also at internal institutional level? Is there a general security and data protection policy that also encompasses VIS purposes? If applicable, which are the internal procedures that provide for using and sharing data?
Q 5	Did the DPAs receive complaints about the competence of the institutions?

Annex II. Second questionnaire on access of law enforcement authorities to VIS data

Questions for the national access point(s)	
Q 1	Are there any other authorities having access to VIS data in addition to those included in the Declaration? If yes, is their access in accordance with Article 5 of the VIS Council Decision?
Q 2	Please provide the list referred to in Article 3(5) of Council Decision 2008/633/ JHA, showing the operational units in the designated authorities authorised to access the VIS via the central access point(s).
Q 3	Do the designated authorities share VIS data directly or indirectly with other national or international authorities?
Q 4	Do internal policies and plans exist within the institutions with a view to ensuring that VIS data is used appropriately also at internal institutional level? Is there a general security and data protection policy that also encompass VIS law enforcement purposes? If applicable, which are the internal procedures that provide for using and sharing data?
Questions for the DPAs	
Q 5	Did you receive complaints about law-enforcement access to the VIS?
Q 6	Based on your national law, do the authorities designated meet the criteria of Article 2(1)(e) of Council Decision 2008/633/JHA? Do you consider that access is restricted to the operational units that need to use it in accordance with Article 3(6) of Council Decision 2008/633/JHA?

Annex III. Third questionnaire on data subjects' rights

Questions for the national competent authorities	
General questions	
Q 1	How would you appreciate the level of awareness of your staff as regards the obligation to safeguard data subject rights? In case of cooperation with external service providers, how do you ensure that DSR are respected by the subcontractors? Did you also perform controls over quality of the information given to data subjects by the subcontractor?
Q 2	For VIS under Council Decision 2008/633/JHA, can data subjects exercise their rights directly or indirectly through the DPA? What relevant national legal provisions apply?
Information on data subject rights	
Q 3	How are data subjects informed of the collection of data about them? Where available, please provide privacy statements or other information material. Are there any national laws that complement the VIS Regulation?
Q 4	How do you evaluate the means used to inform data subjects' rights? (such as the leaflets on VIS[17]).
Q 5	Did you receive any complaints about the information provided in accordance with the Article 37(2) and (3) of the VIS Regulation?
Q 6	In cases when visas are issued on behalf of another state do you insert different information in the visa application forms?
Procedures for granting the right to access	
Q 7	Please describe the procedures in force for granting the right to access (e.g. formal requirements, time limits for replying, fees, possible exemptions). How many requests have you recorded in accordance with Article 38(1) of VIS Regulation? How is the right of access exercised under Article 14 of VIS Council Decision 2008/633/JHA? Please also provide relevant excerpts of national provisions that do apply and statistics if any.
Procedures for granting the right to correction	
Q 8	Please describe the general procedures in force for granting the right to correction in accordance with Article 38(2) of VIS Regulation and provide statistics (if available).

[17] http://ec.europa.eu/dgs/home-affairs/e-library/multimedia/publications/index_en.htm#0801262489da9f79/c_

Q 9	How is Article 5 of VIS Council Decision 2008/633/JHA applied at national level? Please provide any specific provisions and statistics (if available).
Procedures for granting the right to deletion	
Q 10	Please describe the procedures in force for granting the right to deletion in accordance with Article 38(2) and (4) of VIS Regulation and Article 14(5) of VIS Council Decision 2008/633/JHA.
Cooperation to ensure the rights on data protection	
Q 11	How do the competent authorities cooperate actively to enforce the rights laid down in Article 38(2, (3) and (4)?
Redress mechanisms	
Q 12	In case a request for access/information/correction/deletion is denied, who can the data subject address for a review of the decision? How is Article 38(6) of the VIS Regulation applied in practice and what is the procedure followed?
Q 13	Is the deadline of 60 days as required by the Article 14(6) of VIS Council Decision respected in practice?
Use of rights /Statistics	
Q 14	How many cases of review did you have? If so how were they dealt with in practice?
Q 15	What was the outcome (granted, partially granted, denied) for each of these categories? Which exemptions have been used for granting and denied requests?
Q 16	How long –on average- did it take to supply the final answer to the data subject or rectify data?
Conclusion	
Q 17	What is your assessment of the situation – are the procedures in force satisfactory? If not or only partially, how could they be improved?
Questions for the DPAs	
Q 18	Do you assess that competent authorities know about their obligation(s) related to data subjects' rights? Do you think that the level of information provided to the applicants is sufficient? Please also provide relevant excerpts. Do you consider the level of information provided about the fact that the VIS data will be also available for law enforcement purposes appropriate?

Q 19	How would you evaluate the outsourcing in the sense of respecting data subjects' rights?
Q 20	How many requests did you receive under Article 39(2) of VIS Regulation? Do you have specific procedures on this? How do you evaluate the level of cooperation with the other Member States authorities? If applicable, please provide the procedure followed when applying the Article 39(3) and statistics (if available).
Q 21	What is your assessment of the general situation - are the procedures in force satisfactory? If not or only partially, how could they be improved?