VIS SCG

Report on training on data protection and data security to staff with access to the VIS

November 2019

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 as completed by Regulation 2008/767/EC of 9 July 2008[1] ('VIS Regulation'). The VIS first became operational in October 2011.

The VIS Regulation sets out which data shall be included in the database at the various stages of processing a visa (application, issuing, discontinuation of examination, refusal, annulment/revocation, extension; Articles 9-14). Apart from data on the visa application (such as planned travel itinerary, inviting persons, etc.), it also includes a photograph of the applicant and fingerprints (Article 9 (5) and (6)).

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, to 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. This data can be accessed by authorities issuing visas, e.g. consulates of Member States (Article 15), by checkpoints at the Schengen border 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).

In specific cases, national law enforcement authorities and Europol may request access to data entered in the VIS for the purpose of preventing, detecting and investigating terrorist and criminal offences. The procedures for such consultations are established in Council

[1] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60.

Decision 2008/663/JHA[2] ('VIS Decision'). These consultations are carried out via central access points in the participating countries and by Europol.

The lawfulness of the processing of personal data in the VIS by the Member States shall be monitored by the national Data Protection Authorities ('DPAs') (Article 41) and the European Data Protection Supervisor ('EDPS') is in charge of checking the compliance of eu-LISA (Artide 42). In order to ensure a coordinated supervision of the VIS and the national systems, Artide 43 establishes the VIS Supervision Coordination Group ('VIS SCG').

A large number of national competent authorities are designated to access the VIS; they may use the system in different capacity and for specific purposes. In doing so, there are always risks of misuses of the system which can have important consequences for data subjects whose data are in the VIS. In order to avoid such misuses, staff of the competent national authorities need to receive specific training related to data protection, including data security. In June 2017, the VIS SCG therefore decided to further explore the training provided to staff of those authorities on data protection.[3]

2. Legal background

In accordance with 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. Member States shall also ensure that each authority entitled to access VIS data takes the measures necessary to comply with the VIS Regulation and cooperates, where necessary, with the national DPA (Article 35).

In accordance with Article 3(2) and 3(3) of the VIS Decision, Member States shall designate the authorities that are authorised to access VIS data for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Every Member State shall keep a list of the designated authorities and central access point(s) and every Member State shall notify in a declaration to the Commission and the General Secretariat of the Council their designated and central access point(s) authorities.[4] Moreover, according to Article 3(5), each Member State shall keep at national level a list of the operating units within the designated authorities that are authorised to access the VIS through the central access point(s).

In accordance with Article 28(5) of the VIS Regulation, before being authorised to process data stored in the VIS, the staff of the authorities having a right to access the VIS shall receive appropriate training about data security and data protection rules and shall also be informed

[2]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, 13.8.2008, p. 129).

[3]https://edps.europa.eu/sites/edp/files/publication/17-08-08_summary_report_10th_vis_scg_meeting_on_13_june_2017_en.pdf

[4] Declarations concerning Member States' designated authorities and central access point(s) for access to Visa Information System data for consultation in accordance with Article 3(2) and 3(3) respectively of Council Decision 2008/633/JHA (2013/C236/01).

of any relevant criminal offences and penalties. Article 8(8) of the VIS Decision provides the same obligation to provide training to staff of the law enforcement authorities having a right to access the VIS.

Furthermore, Article 38(3) of Regulation (EC) No 810/2009[5] ('the Visa Code') provides that Member States' central authorities shall provide adequate training to both expatriate staff and locally employed staff and shall be responsible for providing them with complete, precise and up-to-date information on the relevant Community and national law.

3. Content of the questionnaire & Methodology

The Group adopted a questionnaire on the training on data protection provided to staff of authorities having access to the VIS following its meeting of 13 June 2017, which was subsequently sent to all Member States.[6] This questionnaire is divided in two parts: the first is addressed to national competent authorities, while the second aims at understanding the national DPAs' involvement in the matter.

The full questionnaire is reproduced in Annex I to this Report.

4. Analysis of answers

Answers to the questionnaire were collected from June 2018 to May 2019. This Report is based on the answers to the questionnaire from twenty-four countries. Out of the respondents, two members did not provide answers to the questionnaire. Moreover, out of the respondents, some members only partially responded to the questionnaire.

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.

4.1. Questions for national competent authorities

***Q1**. Are there any procedures in place to ensure that each staff member (i.e. in the Ministry of Migration, the Ministry of Foreign Affairs, the users in consulates, central access points dealing with request for access to VIS data for law enforcement purposes) having direct access to the VIS has received appropriate training about data protection rules, including data security, prior to such access?*

- *If yes, who is responsible for making sure the access is only given after the training and are there any kind of records of these trainings being provided (e.g. written record)?*
- *If not, when is the training about data protection rules provided to staff?*

[5] 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), OJ L 243, 15.9.2009, p. 1.

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

The majority of Member States informed that they have procedures in place to ensure that staff members having direct access to the VIS have received appropriate training on data protection rules. A few Members do not provide for specific training, as staff would not be able to have direct access to the VIS or this is simply not available. When such training to staff having direct access to the VIS is provided, the national competent authorities generally provide the training.

***Q2**. Are there any procedures in place to ensure that each staff member of the operating units within the designated authorities that are authorised to indirectly access VIS data through the central access point for law enforcement purposes, has received appropriate training about data protection rules, including data security, prior to such access?*

- *If yes, who is responsible for making sure the access is only given after the training and are there any kind of records of these trainings being provided (e.g. written record)?*
- *If not, when is the training about data protection rules provided to staff?*

With regards to the procedures in place which ensure that each staff member of the operating units within the designated authorities that are authorised indirect access to the VIS, most Member States do not have such procedure in place. The reasons is the fact that staff may not have indirect access in the first place or simply because certain procedures still need to be put in place.

When such training to staff having direct access to the VIS is provided, the national competent authorities generally provide the training.

***Q3**. Who is in charge of providing the training about data protection rules to the staff?*

As regards the person who is in charge of providing the training on data security and data protection to staff having access to the VIS, several Member States identified the DPO of the responsible authority as the main responsible person for the trainings. Other Members referred to staff from the Ministry of Foreign Affairs, to the Directorate for Immigration, to the Consular Service and to the State Border Guard as the providers of trainings.

***Q4**. Is the Data Protection Officer of the national competent authority involved in any way in the setting up or the provision of such training?*

Concerning the involvement of data protection officers within the setting up of the training provided to the staff having direct or indirect access to the VIS, the majority of Member States involve the DPO of the national competent authority. Certain authorities are planning to involve the DPO of national competent authorities in the near future, while for others this information was still not available.

***Q5**. How long does the training about data protection rules last?*

The duration of the trainings for staff having access to the VIS vary considerably among the Member States: some last a few hours (between 1 and 16 hours), while others last up to a few days (between one and nine days). For some Members, a specific duration could not be specified as these are horizontal trainings given during a specific period.

***Q6**. Please describe the content of the training about data security and data protection rules (i.e. program of the training and main topics).*

Concerning the content of the training about data security and data protection rules provided to staff with access to the VIS, the majority of Member States largely focuses on general information about the data protection principles and the GDPR, together with specific training on data protection within the VIS, security measures and data subjects' rights. A few Member States particularly concentrate on the VISA policies.

***Q7**. Is there any later evaluation to validate that staff members with direct access to the VIS have sufficient knowledge of data protection rules?*

Only in some of the Member States, staff members with direct access to the VIS are assessed on their knowledge of data protection rules. The rest of the Members were not aware of such information or simply do not provide for an evaluation of such knowledge.

***Q8**. Is there any sort of continuous training about data protection rules, including data security, provided to the staff?*

- *If yes, how often are such trainings provided to the staff?*

Most of the Member States provide for a continuity in training, while others have a series of reminders and awareness-raising activities. In substance, the Member States providing for training may vary in substance and timing, usually once every few months or whenever necessary, around twice a year, once a year or even once every four years.

***Q9**. Is there any internal document about data protection rules, including data security, available that staff members could consult at all times?*

The great majority of the Member States stated that there are internal documents about data protection rules, including data security, available at any time for staff members' consultation. By way of example, such documentation could be included in handbooks, published on websites/ intranets, included in internal code of conducts, or published on leaflets and books.

One Member State stated that no such document is available.

***Q10**. Are there any procedures in place to ensure that each staff member having direct access to the VIS is informed of any relevant criminal offences and penalties in cases of misuses?*

- *If yes, are there any kind of records of this information being provided to staff?*

Concerning the internal documentation in place about data protection rules, answers to this question revealed that, in the majority of Member States, authorities have specific procedures in place to ensure that each staff member with direct access to the VIS is informed of any relevant criminal offences and penalties in cases of misuses. The practical ways in which this information is provided vary throughout the Member States: in some instances, such information is given through the training programs themselves, while in some other cases such information is given through the contract or confidentiality agreements. With regard to records of this information being provided to staff, some Member States answered that there are no records available, while some others stated that records can be produced (e.g. through the lists of staff members who participated in trainings, or through system logs).

A minority of the Member States replied that there are no specific procedures with regard to this issue. However, some of these Member States also pointed out that this kind of information is included in the more general information provided with regard to data protection law within trainings or employment contracts.

***Q11**. Is there any specific training about data protection rules, including data security, provided to staff members of central access points dealing with requests for access to VIS data from other designated authorities for law enforcement purposes?*

- *If yes, please describe the content of this training and its specificities?*

With regard to specific training about data protection provided to staff members of central access points dealing with requests for access to VIS data from designated authorities, some Member States informed that they provide such training whereas others do not offer it. Generally speaking, such trainings include information on data protection principles as well as specific topics relating to law enforcement access to VIS data, and are provided in person and/or via manuals and handbooks.

***Q12**. What is your assessment of the situation – are the trainings in place satisfactory?*

- *If not or only partially, how could they be improved?*

Generally, the trainings in place were considered to be quite satisfactory. At the same time, many Member States highlighted a need for improvement.

Some Member States also mentioned that the training procedures are actually being assessed/updated, thereby stressing that there is an ongoing attention to this topic. It should also be noted that some Member States called for further unification of data protection training rules at EU level.

The possible improvements that were mentioned included additional investments, the need for the trainings to take place more often and/or be updated on a regular basis, e-training possibilities, topic-oriented trainings, and checks on the misuse of the system.

4.2. Questions for national Data Protection Authorities

***Q13**. Are you involved in any way in the provision of training about data protection rules to staff members of relevant authorities?*

Several DPAs informed that they are involved in the provision of training about data protection rules to staff members of national competent authorities (e.g. by directly providing lectures or by participating in the development of e-learning courses).

Other DPAs replied that they are usually not involved or that they are only involved in part or when needed.

***Q14.** How do you check that the obligation to provide appropriate training to staff of the authorities having a right to access the VIS is complied with in practice?*

The great majority of DPAs informed that compliance with the obligation to provide appropriate training to staff of the authorities having a right to access the VIS is checked through inspections, planned checks and audits.

***Q15**. Do you assess that relevant national competent authorities know about their obligation to provide training about data protection rules, including data security, to staff members using VIS data?*

With regard to national competent authorities' awareness of their obligation to provide data protection training, most DPAs answered that national competent authorities generally know about their obligation to provide training about data protection rules, including data security, to staff members using VIS data.

Some DPAs specified that this aspect is one of the issues covered by their periodic checks and inspections.

***Q16**. What is your assessment of the situation – are the trainings in place satisfactory?*

- *If not or only partially, how could they be improved?*

Most DPAs assessed the trainings in place as being overall satisfactory; at the same time, the majority of DPAs highlighted that there is room for further improvement, including: the update and further development of training materials, the increase in the amount of training sessions carried out and in their regularity, the introduction of e-learning modules, a greater involvement of DPOs and DPAs, a specific focus on practical cases and examples.

5. Conclusions & Recommendations

Looking at the outcome of this questionnaire, the VIS SCG welcomes the overall satisfactory situation with regard to the training on data protection provided to staff having access to the VIS and encourages the Member States to further improve and regularly update their programs, both in terms of organisation and in terms of content.

While the majority of respondents informed that there are procedures in place to ensure that staff members having access to the VIS receive appropriate training on data protection and security, there are still some Member States in which such training is not available. The VIS SCG encourages all Member States to ensure that such trainings are in place for all staff having direct or indirect access to the VIS.

As far as improvements are concerned, a greater cooperation among Member States should also be encouraged, in terms of exchanging good practices and experiences. In addition, the answers to the questionnaire revealed that the substance and regularity of trainings vary widely: improving the frequency of trainings and keeping the contents up to date should be one of the priorities. Interestingly, some Member States called for greater unification of data protection training rules at EU level.

Brussels, 27 November 2019

Annex 1: Questionnaire

Part 1 : Questions for national competent authorities

1. Are there any procedures in place to ensure that each staff member (i.e. in the Ministry of Migration, the Ministry of Foreign Affairs, the users in consulates, central access points dealing with request for access to VIS data for law enforcement purposes) having direct access to the VIS has received appropriate training about data protection rules, including data security, prior to such access?

- If yes, who is responsible for making sure the access is only given after the training and are there any kind of records of these trainings being provided (e.g. written record)?

- If not, when is the training about data protection rules provided to staff?

2. Are there any procedures in place to ensure that each staff member of the operating units within the designated authorities that are authorised to indirectly access VIS data through the central access point for law enforcement purposes, has received appropriate training about data protection rules, including data security, prior to such access?

- If yes, who is responsible for making sure the access is only given after the training and are there any kind of records of these trainings being provided (e.g. written record)?

- If not, when is the training about data protection rules provided to staff?

3. Who is in charge of providing the training about data protection rules to the staff?

4. Is the Data Protection Officer of the national competent authority involved in any way in the setting up or the provision of such training?

5. How long does the training about data protection rules last?

6. Please describe the content of the training about data security and data protection rules (i.e. program of the training and main topics).

7. Is there any later evaluation to validate that staff members with direct access to the VIS have sufficient knowledge of data protection rules?

8. Is there any sort of continuous training about data protection rules, including data security, provided to the staff?

    - If yes, how often are such trainings provided to the staff?

9. Is there any internal document about data protection rules, including data security, available that staff members could consult at all times?

10. Are there any procedures in place to ensure that each staff member having direct access to the VIS is informed of any relevant criminal offences and penalties in cases of misuses?

    - If yes, are there any kind of records of this information being provided to staff?

11. Is there any specific training about data protection rules, including data security, provided to staff members of central access points dealing with requests for access to VIS data from other designated authorities for law enforcement purposes?

    - If yes, please describe the content of this training and its specificities?

12. What is your assessment of the situation – are the trainings in place satisfactory? If not or only partially, how could they be improved?

Part 2: Questions for national DPAs

13. Are you involved in any way in the provision of training about data protection rules to staff members of relevant authorities?

14. How do you check that the obligation to provide appropriate training to staff of the authorities having a right to access the VIS is complied with in practice?

15. Do you assess that relevant national competent authorities know about their obligation to provide training about data protection rules, including data security, to staff members using VIS data?

16. What is your assessment of the situation – are the trainings in place satisfactory? If not or only partially, how could they be improved?