VIS SCG

# Common Inspection Plan

# For the Visa Information System (VIS)

Adoption February 2024

Corrigendum May 2024

# Contents

# Introduction

According to the Working Program 2019-2021 of the Visa information system Supervision Coordination Group (VIS SCG), one of the activities was to develop a Common Inspection Plan. The purpose was to provide an assistance tool for supervisory authorities (SAs) to perform their supervisory role. It should also provide for a common approach to the inspections, allowing a better analysis and comparison of results.

This document provides relevant support for SAs in carrying out inspections, though always as a reference text still allowing flexibility and tuning at national level, according to the specifics of the federal structures, national procedures or methodologies.

The Common Inspection Plan is a dynamic document. It is therefore open to constant adjustment and consolidation as the VIS SCG sees fit.

## Scope

This document provides a set of questions (checklist) and advice, considered pertinent when inspecting the data processing of the Visa information system (VIS) from a data protection perspective. It follows the requirements of Regulation (EC) No 767/2008 (VIS Regulation)[1], Regulation (EC) No 810/2009 (Visa Code) and the Council Decision 2008/633/JHA (VIS Decision)[2].

It is based on the "Common Audit Framework - Part II – Alerts Module - Joint Model for Inspecting SIS II Alerts", which was created by the SIS II Supervision Coordination Group (SIS II SCG). In order to facilitate the mapping between the two frameworks, a similar structure has been used.

The document is separated in different sections, concerning the VIS stakeholders that can be found at national level (e.g. data controller, data processor, supervisory authority, and external service providers).

The framework took into account the previous recommendations made in the context of Schengen Evaluations (SCHEVAL) in different Member States concerning VIS. The recommendations have been adapted in the form of questions, to ensure that there are no specific references to the Member States concerned.

The legal bases in each section refer only to specific provisions of the VIS Regulation and the Visa Code.

Furthermore, according to Article 36a of the VIS Regulation, the general data protection rules of Regulation (EU) 2016/679 and Directive (EU) 2016/680 apply to the respective context.

## Out of scope

This document does not cover specific aspects of information security management. These aspects were previously addressed in the "Data security module for large scale IT Systems" of the "Common inspection framework", developed by the SIS SCG Technical Expert Subgroup[3].

[1] Version after amendment by Regulation (EU) 2021/1134.
[2] For the complete list of legislation in scope, please consult the section "Relevant legislation".
[3] The SIS II Technical Expert Subgroup prepared a data Security module as part of a Common Framework for Inspection, which could help SAs perform inspections on SIS, VIS and Eurodac.
The scope of the Data Security module is limited to Information Security and IT Security in the context of the large-scale IT system mentioned previously.
The module is based on ISO 27001:2013 and ISO 27002:2013 standards.

## Relevant legislation

**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)**
(Lays down the purpose, functionalities and responsibilities for the VIS, as well as the conditions and procedures for the exchange of short-stay visa data between Member States to facilitate the examination of applications for short-stay visas and related decisions)

**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 **(VIS Decision)**

**Regulation (EC) No 810/2009** of the European Parliament and of the Council of the Council, of 13 July 2009 establishing a Community Code on Visas **(Visa Code)**
(Sets out the rules on the registration of biometric identifiers in the VIS)

**Regulation (EU) 2016/679** of the European Parliament and of the Council, of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**GDPR**)

**Regulation (EU) 2018/1861** of the European Parliament and of the Council, of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 **(Revision of the SIS regulation)**

**Regulation (EU) 2021/1134** of the European Parliament and of the Council, of 7 July 2021 **(Revision of the VIS Regulation and of the Visa Code)**
(Amends Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System)

# Questions to the Member State authorities

## A. Data controller and data processors

*Specific legal provisions: Article 28 (2) VIS Regulation*

1. Which is the central authority for the National Central Visa information system (NS-VIS)?
2. Is the central authority the data controller for VIS? If not, which is the data controller?
3. Is there a joint data controllership for VIS?
    a. If so, are the responsibilities clearly defined?
    b. Can the arrangement be provided? (Article 26 GDPR)
4. Are there any public bodies acting as data processors for the NS-VIS? If so, which national bodies and for which purposes?
5. Is the division of tasks and responsibilities between all authorities involved in the visa application and issuance procedure with regard to the processing of personal data in the VIS clearly defined and documented?
6. Are there any outsourcing private providers acting as data processors in relation to NS-VIS data? If so, which private companies and for what purposes are they involved?
7. Is there a contract between the data controller and each data processor?
8. How does the data controller ensure that there is sufficient supervision of the data processors and that data protection and security requirements are being implemented?
9. How are the DPOs of the competent authorities involved in the relevant operations related to the processing of personal data in the VIS, including self-auditing?
10. Do you have a national legal basis for local warning lists? What are the requirements for setting up and keeping local warning lists, e.g. regarding data retention, access rights, data subject rights, logging?

## B. VIS data and national copies

*Specific legal provisions: Article 28 (4) VIS Regulation*

11. What is the VIS architecture for the Member state?
12. How is access to the central visa information system (CS-VIS) provided in the Member State (i.e., are the queries directed to the CS-VIS directly, or to national copies)?
13. Is there more than one national copy of CS-VIS?
    a. If so, how many copies are there, and are they partial or full copies?
    b. Which authority stores and/or manages each copy?
    c. What is the purpose of each technical copy?
    d. Is there an up-to-date inventory of these copies?

14. What procedures are in place to ensure that the technical copies are consistent with the NS-VIS? How often does the synchronization take place?
15. Is remote access to the NS-VIS and/or to other national copies implemented using mobile devices?
    a. If so, for what purpose?
    b. Is there a security policy in place for lost or stolen for remote access devices?

## C. Authorities having access to VIS

*Specific legal provisions: Article 6 VIS Regulation*[4]

16. Are there national legal acts regulating the access to the VIS?
17. Which authorities have access to the VIS? Do they correspond to the list published in the Official Journal of the European Union pursuant to Article 6 (3) of the VIS Regulation and Article 3 of the VIS Decision?
18. Do the authorities fulfil the legal tasks mentioned in the VIS Regulation and the Council Decision and are they in conformity with national law?
19. Is it possible to consult the VIS simultaneously with other national systems by using a single search interface? Which authorities have this possibility, in what context, and for what purpose?

## D. Access to the VIS for law enforcement purposes

*According to VIS Decision* - Note: The VIS Decision will be repealed by the Regulation 2021/1134, Articles 10 and 12

*Specific legal provisions: Articles 22l and 22t VIS Regulation*

20. Does the Member State keep a list, at the national level, of the operating units within the designated authorities authorized to access the VIS through the central access point? Is the list kept centrally or separately by each authority?
21. How many central access points operate in the Member State? Have all central access points been notified to the Commission and the General Secretariat of the Council?
22. What are the procedures for making a reasoned written or electronic request to a central access point?
23. Under the existing procedures, is it possible to make a single reasoned request to carry out several searches?
24. How does the central access point(s) verify that the conditions for access are met? Are there functional solutions implemented to support in the decision-making process?

[4] Amended by Regulation 2021/1134: Chapters II and III, Articles 45a, 45b, 45c, 45d, and 45e - partly not yet in force

25. How long does it usually take the central access point(s) to carry out the ex-post verifications? Is the deadline defined in the applicable provisions?
26. If the outcome of the ex-post verification indicates that the conditions have not been met, what action will be taken by the central access point(s)?
27. Are there any statistics available on what percentage of requests are emergencies?
28. Have all requests made by designated authorities met the conditions set out in the Article 5(1) VIS Decision[5]?
29. Have the conditions set out in Article 22o VIS Regulation been checked for all requests from designated authorities[6]?
30. Have all searches been limited to the data specified in Article 2 of the VIS Decision[7]?
31. Is the data collected under the Decision processed only for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and other serious criminal offences?
32. Have data obtained from the VIS pursuant to this Decision ever been transferred or made available to a third country or an international organization? Were such transfers made exclusively for the purpose of the prevention and detection of terrorist offences and of other serious criminal offences and under the conditions set out in Article 22o (1) of the VIS Regulation as amended by Regulation 2021/1134, subject to the consent of the Member State which entered the data in the VIS, and in accordance with the national law of the Member State transferring or making available the data?
33. Does the Member State keep records of such transfers? Please provide a copy.
34. Is VIS data being kept in national files? (Article 13 VIS Decision)
    a. Under what circumstances and for how long?
    b. Is this procedure regulated? Is there any documentation?
35. Are all data processing operations resulting from access to the VIS for consultation pursuant to the Decision recorded (logged)?
    a. Does the log file contain the information specified in the Article 22s (3) of the VISA Code as amended by 2021/1134?
    b. Are the logs only used to monitor the lawfulness of the processing and to ensure data security?

[5] New Article 22o of VIS Regulation, as amended by Regulation 2021/1134 - not yet in force
[6] New Article 22n (1) of the VIS regulation, as amended by Regulation 2021/1134
[7] New Article 22o (3) of VIS Regulation, as amended by Regulation 2021/1134 - not yet in force

## E. Visa application request

*Specific legal provisions: Chapter II (Articles 9-17) Visa Code*[8]

36. How can data subjects apply for a visa?
37. Regarding the method(s) for visa application:
    a. Are they paper-based? Electronically, via website? Other?
    b. Which entity is responsible for managing the application?
    c. What categories of data are processed?
    d. How long is the data stored?

## F. Data subject rights (information, access, rectification, and deletion)

*Specific legal provisions: Articles 37 and 38 VIS Regulation*

*Information about the VIS system*

38. When information is provided to the data subject, does it contain all the information required by Article 37 of VIS Regulation?
39. When providing information to the data subject, is it indicated to which authority should individuals address themselves in order to exercise their rights and which authority will deal with these requests?
40. Does the standard visa application form provide sufficient information on the following:
    a. Identification of the different data controllers that process personal data as part of the national visa system.
    b. Information about the different authorities that process personal data as part of the national visa system.
    c. Information about the data processing prior to entering their personal data in the visa application form.
41. If online application forms are used, do the fields of the electronic visa application form correspond to the fields of the paper visa application form (as defined in Annex I of the EU Visa Code)?
42. Are the persons (other than the visa applicant) whose data are processed in the VIS (e.g. the person inviting a visa applicant) provided with the same information on the data processing activities than the visa applicant (including information on the controller, the purpose, the data retention period, the recipients, the right of access and the mandatory nature of the processing for the examination of the application)?

[8] Visa Code amended by Regulation 2021/1134 - not yet in force

*Information on exercise of rights*

43. How can individuals exercise their right of access, to rectification, completion, erasure and restriction of processing VIS data (e.g. form, post letter)? Is it possible to submit a request electronically?
44. Are data subjects provided with clear information about:
    a. The authorities to which data subjects should address their requests for access, rectification and deletion of VIS data?
    b. Where to send such a request?
    c. What information should be provided on the request?
    d. Fees concerning the right of access? In what situations are fees charged for the handling of data subjects' requests?
    e. Limits on the number of access requests a person can make?
    f. How can an appeal/complaint be lodged against a decision on a request concerning the data subject's rights?
        i. Information on whom to contact and where to send such an appeal?
        ii. In which language will a decision be taken on an appeal concerning a request by a data subject in the VIS? Are data subjects, who do not speak the local language, provided with an informal English version of the SA's decision?
    g. Easily accessible model letters for exercising the rights for data subject and for appeals?
    h. Is the exercise of the rights of data subject facilitated by accepting simple copies of documents proving the identity of the person and only requiring a certified copy only when there is doubt about the identity of the person?
45. With regard to the way the information on the exercise of rights is provided:
    a. How is the information published? (Website, leaflets?)
    b. Is the information comprehensive, easy to find, and updated?
    c. Is the information available in English?
    d. Can individuals submit their request and receive answers in other languages, especially in English?
    e. Is there any printed information (leaflets/signs etc.) that is made available to data subjects/the public in more accessible places, such as the premises of police stations, border control areas, consular offices, airports?
46. Does the data controller website provide:
    a. Information on VIS data subjects' rights accessible to the public?

b. Templates for exercising the rights of VIS data subjects?

47. In cases of refusal or restriction of access, including the omission of the reasons for the refusal or restriction, are data subjects informed about the possibility to exercise their rights through the competent supervisory authority?
48. Are there any national legal dispositions regulating data protection rights with regards to the VIS?
    a. If so, does the legislation provide for additional or different requirements to those of the VIS legal framework? If yes, in what way?
    b. Is there a time limit in national law for responding to VIS data subject requests?
49. When data subjects receive a reply to their access request:
    a. What information is provided to the data subject? Is a copy of the data provided to data subjects?
    b. Are data subjects only informed that their data are processed in the VIS?
    c. Are data subjects provided with sufficient information about the complaint mechanisms and judicial redress?
    d. Are replies provided to data subjects' requests in the same format as they were requested?
50. What is the procedure in place for data subjects to have unlawfully stored data relating to them deleted?
51. Does the national competent authority have an internal policy for handling requests for access, rectification and deletion?
    a. How is it ensured that the time limit laid down in the VIS legal framework or in national legislation is respected when handling requests from data subjects?
    b. Are the procedures for assessing data subject's requests, in particular when limiting the right of rectification or erasure, made clear to the data subject?
        i. Is this in line with the applicable Union and national law?
52. Do the involved authorities have clear (internal) procedures defining the responsibility of dealing with VIS data subjects' rights?
53. Is the entire process for accessing, rectifying or deleting data documented? If so, how?
54. Are there statistics on the number of requests by individuals for the exercise of data protection rights?
55. Is there a designated body/department to deal with requests from individuals?
    a. How many people deal with such requests?
    b. Is representation guaranteed in case of absence?

## G. Data input

*Specific legal provisions: Article 28 VIS Regulation*

56. Which national competent authorities input data directly in the CS-VIS?
57. Which national competent authorities input data in the CS-VIS through national copies?
58. Are there national legal acts regulating the insertion of data?
59. What are the source systems for each visa application? (e.g. consulates, embassies)
60. Is the data transferred from the source systems to VIS automatically, manually, or both? Please describe the data flow from initial data entry to transmission to CS-VIS.
61. Are the source databases and the NS-VIS linked? If so, is the NS-VIS updated in real time or batched according to new data entered in the source database?

## H. Biometric data

*Specific legal provisions: Articles 4 (14), 9 (6), and 45 (3) VIS Regulation, Article 13 Visa Code*

62. How are fingerprints enrolled and accessed?
63. How is the quality of biometric data guaranteed?
    a. Is the quality of the fingerprint checked before it is uploaded into the VIS?
    b. How are the problems related to the quality of biometric data (blank references, duplication of information, generally poor quality of data) addressed?
64. Are there any missing facial images and/or missing fingerprint sets?
    a. Could you explain the reasons for this issue?
    b. Could you provide statistics?
    c. What are the procedures to address this issue?
65. What are the procedures when the enrolment of biometric data is not successful?
66. What are the procedures for access to searches with fingerprints at external border crossing points[9] and within the territory of the Member State[10]?
67. Are there statistics about the quality of biometric controls?
    a. Is the percentage of the unsuccessful recordings available centrally and to end users?
    b. How are facial images enrolled and accessed?
    c. Is the quality of the photo checked before it is uploaded to the VIS?

[9] Article 18 of the VIS Regulation
[10] Article 19 of the VIS Regulation

## I. Identification and authentication of users

*Specific legal provisions: Articles 28 (4) and 32 (2) Visa Regulation*

68. Is there a common identity management policy for all VIS users?
    a. If so, which authority is responsible for it?
    b. Is it the NS-VIS data controller, or are there different policies?
    c. If the latter, identify the different practices and the respective authorities and contexts involved.
69. What is the role of the NS-VIS data controller in granting access to the VIS?
    a. Does the controller have effective first-hand control over access to the system?
    b. How and by which authorities are access rights managed?
70. Does the authentication system allow the direct identification of an end-user or is the access granted to a generic user (e.g. web service)?
71. If access is granted to a generic user, how are individual users identified?
    a. Are users provided with specific credentials to access the VIS?
    b. How is access controlled and by whom?
72. How is it ensured that access to the VIS is only granted to users who really need it for the performance of their tasks?
73. If there is a single search interface integrating the search of the VIS, how is it ensured that users accessing the VIS through this mechanism also have the appropriate authorization to consult the VIS on a need-to-know basis?
74. How is it ensured that only data necessary for the performance of their tasks is accessed?

## J. Staff training

*Specific legal provisions: Article 28(5) VIS Regulation, Article 38 (3) Visa Code*

75. Did the staff of the authorities having a right to access to the VIS receive adequate training on data security and data protection rules?
    a. Did the training include information on relevant criminal offences and penalties?
    b. How soon after starting work do newcomers receive appropriate training and when do they have access to the systems?
76. Did the training cover all staff using the VIS from all competent authorities concerned?
    a. If not, who received the training?
    b. How is it ensured that newcomers receive the necessary data protection training before starting to use the VIS?

77. Does the training include information on any relevant criminal offences and penalties in case of breach of data protection rules, including security rules?
78. Has the Supervision Authority contributed in any way to the training sessions? If so, how?
79. Has the DPO been directly involved in the development and provision of data protection training to staff including those provided to embassies/consulates?
80. Is the staff training documented? If so, how?

## K. Application/business logs

*Specific legal provisions: Article 34, and 32 (2) VIS Regulation, and Article 16 VIS Decision*

81. Which entity is responsible for the storage and management of the logs and for ensuring their integrity and confidentiality?
82. Is there a single policy at national level regarding the VIS logging activity or are there different policies or practices?
83. Regarding the keeping of records:
    a. What actions are logged (access, creation, modification, search, consultation, deletion)?
    b. What is the content of the log files and do they comply with Article 34(1) of the VIS Regulation and Decision?
84. Do the logs identify the purpose of the access?
85. How are logs technically managed?
86. Is it possible to identify the user with the help of the log file?
87. What is the retention period of the logs?
    a. What were the criteria for the setting of the retention period?
    b. Are any logs kept for longer than the legal retention period?
88. If the Member State does not use a national copy, how is it ensured that each access to VIS data and each exchange of VIS data is logged?
89. Where are logs stored? Centrally by the data controller or with the accessing authorities?
90. Who has access to the logs, by each authority? What measures are in place to prevent unauthorized access?
91. Have there been cases where the logs showing access to VIS data and all exchanges of VIS data have been used for self-monitoring of compliance with data protection rules?
92. Are these logs regularly checked/inspected?
    a. By whom?
    b. Are there any reports on this analysis?
    c. How long are these reports kept?

d. Are there procedures in place in the event that abusive access is detected?

## L. Prior consultation of central authorities of other Member States and use of VIS for consultation and request for documents

*Specific legal provisions: Articles 4(5), 22, and 31 VIS Code, and Article 16 Regulation (EC) No 767/2008*

93. Has the Member State consulted the central authorities of another Member State, or have other Member States consulted the local central authority, during the examination of applications lodged by nationals of specific third countries or specific categories of such nationals?
    a. If so, how many consultations have been made in the past years?
    b. How many of the consultations were made by consulates?
    c. How long did it take to answer, if at all? (Article 22(2) envisages that a reply should be given within 7 calendar days, and that the absence of a reply within that deadline means the Member State has no grounds for objecting the issuing of visa)
    d. If there has been a withdrawal of any of the applications, how has this been communicated to the European Commission?
    e. When receiving consultations, how is the personal data therein handled?
    f. In which cases is prior consultation with the authorities of other Member States mandatory?
    g. In which cases must the authorities of other Member States be informed of visas issued?
94. In what situations are other Member States consulted and information/documents exchanged?
    a. What types of data are generally exchanged?
    b. How is the information received stored?
    c. When is this data deleted?

## M. Consular posts

*Specific legal provisions: Article 28 VIS Regulation, Articles 37-43 Visa Code*

95. How do consular posts access the VIS? Do they have access to the VIS directly, or do they access via technical copies?
96. Do consular posts copy VIS data into their own records? If so, for which purpose?
97. In cases where consular posts access the VIS via one or more copies of the NS-VIS stored either at Member State level or at consular post level, how is the data updated to be consistent with the NS-VIS?
    a. How often is the synchronization carried out?
    b. Is this update done simultaneously in all consular posts?

98. Do staff temporarily assigned to a consular post and recruited from nationals of that country have access to the VIS?
    a. If so, are they subject to security checks?
    b. Is this staff trained?
99. What is the procedure when a search indicates that data on the applicants are recorded in the VIS?
100. Is data transmitted to/from consular posts in encrypted form?
101. Is the controller aware of which countries and which consular posts use the services of external service providers (ESPs)? Does the controller know who these ESPs are and what services they provide?
102. How does the Member State as controller monitor the compliance of the processing of visa applications by external service providers with data protection requirements? Provide evidence of supervision.
103. How often does the Member State check the processing of data by external service providers?
104. How often are on-the-spot checks carried out in accordance with Article 43(11) of the Visa Code? Who (which organisational unit) carries out the on-site verification?
105. Are reports or other documentation produced on the experience of the audits?
106. How do you check the adequacy of data transmission (encryption) from external service providers to consulates?
107. Do external service providers transmit data to consulates on paper?
108. How do you check the compliance of paper-based data transmission with data protection requirements?
109. What data are processed and transferred by the ESPs?
110. What are the rules for collecting and transmitting biometric identifiers?
111. What are the rules regarding the deletion periods of the data recorded by the ESPs?
112. Does the contract concluded with the ESPs provide for data erasure rules?
113. How is the training of the providers' staff ensured?
114. How is the provision of the information required by Article 37 of the VIS Regulation to visa applicants by the external service provider verified?
115. How is the adequacy of the technical and organisational security measures taken by the ESPs verified?
116. What problems have been encountered in working with ESPs?
117. Has there ever been a case where a contract with an ESP was terminated because its service did not comply with the data protection requirements?

118. Has a complaint from a data subject been received by the consulates or directly by the data protection officer of the competent national ministry in relation to services provided by external service providers?

119. Please provide the latest report sent to the Commission on your cooperation with, and monitoring of external service providers worldwide as referred to in Article 43 (11a) of the Visa Code.[11]

## N. Data quality

*Specific legal provisions: Article 29 (1) VIS Regulation[12]*

120. Is there national legal legislation or policy on the quality of the data to be entered in the VIS?

121. How is the quality and accuracy of VIS data ensured? Is there a documented procedure?

122. Is all available data entered into VIS or only the minimum data required? What criteria are used?

123. How are the different responsibilities allocated if different authorities are responsible for data quality and integrity?

124. Are there audits of the data quality?

   a. Are the audits documented?

   b. Are there statistics?

125. How is it ensured that only the relevant data are uploaded into the VIS when the data are automatically entered into the VIS from a national source system?

126. Which authority receives and analyses the quality reports sent by eu-LISA? How are any problems identified dealt with?

127. Is VIS data further processed, reused or crosschecked with other data? If yes, when and for which purposes?

## O. Statistics

*Specific legal provisions: Regulation (EC) No 767/2008, Article 45a*

The relevant provision (Art. 45a) VIS Regulation will apply from the date set by the Commission by means of an implementing act, but no later than 31 December 2023 according to Art. 11 and 12 of Regulation (EU) 2021/1134

*- A time interval for the statistics to be provided should be determined beforehand (e.g. last 2 years) -*

[11] According to Article 43 (11a) of Visa Code '1 February each year, Member States shall report to the Commission on their cooperation with, and monitoring, as referred to in point C of Annex X, of external service providers worldwide'.

[12] New Article 22a VIS Regulation, as amended by Regulation 2021/1134 - not yet in force

128. How many visa applications were processed under the responsibility of the country's authorities?

129. Number of hits resulting from queries of EU information systems, Europol data or Interpol databases pursuant to Article 9a or 22b, broken down by system or database[13].

130. Number of refused visas, long-stay visas or residence permits, broken down by reason for refusal.

131. For each of these statistics, an indication of the number of applications for each type of visa should be provided.

## P. Exchange of supplementary information by the designated authority

*Specific legal provisions: Articles 9d and 9f VIS Regulation*

The relevant provisions (Art. 9d and f) VIS-Regulation will apply from the date set by the European Commission by means of an implementing act, according to Art. 11 and 12 of Regulation (EU) 2021/1134.

At the time this inspection plan was adopted, the exchange of supplementary information had not yet been in place. Please ensure that the exchange of supplementary information is in place before addressing the following questions.

132. How is the «supplementary information» exchanged between the VIS designated authorities stored? Electronically and/or in manual files? And, how?

133. Under what conditions is the information exchanged stored by the VIS designated authority? In manual and/or digital files?

134. What tools does the VIS designated authority use to exchange information with its partners and contacts? Please describe.

   a. Are those tools exclusively dedicated to the exchange of VIS data?
   b. If not, what are the other purposes for which their use is allowed?
   c. What measures have been taken to secure the exchanges?

135. Who has access to stored information relating to supplementary information?

   a. How does the system record access to stored information concerning the exchanged data, both in manual or electronic data filing systems?
   b. What categories of data are recorded?

136. Is there a written policy or common practice regarding the deletion of the «supplementary information»?

137. When is the «supplementary information» deleted? Is there a clear time limit?

138. Are there specific procedures or rules concerning the storage of «supplementary information» when there is a situation of interlinked alerts? Clarify.

[13] Article 45a (k) of the VIS Regulation

139. In practice, following a request, how long does it take, in average, for supplementary information to be provided? Is there a specific legal provision under national law defining a response time?

## Q. Advance erasure of data

*Specific legal provisions: Regulation (EC) No 767/2008, Article 25*

140. Is there an established procedure for systematically informing the VIS authorities when a person whose personal data are processed in the VIS acquires the citizenship of a Member State?

141. How long does it normally take for the VIS authorities to inform the responsible Member State?

## R. Communication of data to third countries or international organisations

*Specific legal provisions: Regulation (EC) No 767/2008, Article 31*

142. Does the Member State transfer data to third countries or international organisations? Under what circumstances?

# Questions to consular posts/embassies

## S. General questions

*Specific legal provisions: None*

143. What kind of equipment is the consulate provided with in terms of staff and equipment?
144. How many visa cases were assessed in the last two years? What is the refusal rate, and what is the main reason for refusal?
145. What is the average time taken to process a visa application?
146. Which is the procedure for communicating with data subjects? What is the language used in the communications?
147. What is the procedure for submitting applications and requests through a legal representative (verification of power of attorney, etc.)?
148. Is the information on the VIS available on the consular website?
149. Do you have a local warning list? Does the local warning list fulfil the national requirements, e.g. regarding data retention, access rights, data subject rights, logging?

## T. Visa applications

*Specific legal provisions: Chapter II (Articles 9-17) and Title IV (Articles 37-47) Visa Code*

150. What is the procedure for applying for a visa application? Is it documented?
151. What personal data is collected during the application process?
152. What are the rules for accesses to the VIS by local and permanent staff?
153. What types of employment contracts do the staff issuing visas have? Are there specific clauses in the contracts regarding the non-disclosure of personal information known to the staff in connection with their work at the consulate?
154. Are there procedures in place to manage the granting, modification and revocation of authorizations? Describe.
155. Are the assigned authorizations checked regularly?
    a. How often are these checks carried out? By whom?
    b. Do you have a formal procedure for carrying out authorization checks? Provide evidence.
156. What software and equipment are used for the data collection?
157. How does the consular post/embassy system communicate with the national instance?
158. What are the security measures in place?
159. How and where are biometric data collected?

160. Have consular officers, consular administrators, and local staff received training in data protection?

## U. Personal data breaches

*Specific legal provisions: None*

161. Have there been any personal data breaches regarding visas? If so, what action was taken?

162. Is there a personal data breach procedure/policy in place?

163. Are the employees trained to know how to deal with personal data breaches?

164. Do the contracts with ESPs dealing with visas include clauses for reporting data breaches?

## V. Paper visa stickers

*Specific legal provisions: Article 37 (2) Visa Code*

165. How and where are visa stickers stored?

166. Who has access to the visa stickers?

167. What physical security measures are in place to protect stored visa stickers?

168. Is there a procedure for handling and storing visa stickers? Is it documented?

169. How does the consulate keep an account of its stock of visa stickers and register how each visa sticker has been used?

## W. External service providers (ESP)

*Specific legal provisions: Article 43, 44 Visa Code, Annex 10 Visa Code*

170. Are there external providers processing personal data for visa applications?
    a. What is their role?
    b. What personal data do the service providers process, and for what purpose?
    c. Which tasks of the visa issuing procedure were delegated to external service providers (ESP)?
    d. Are there any specific requirements that the external service providers have to fulfil?

171. Is there a contract for this service? (Retrieve copy)
    a. What provisions does it have about the protection of personal data[14]?
    b. Are standard contracts used?
    c. Does the contract concluded with the external service provider contain detailed provisions on checks by the Member State (Consular Service) and possible sanctions?

[14] See the VIS SCG document "Analysis of the data protection law applicable to "External Service Providers" (ESPs) and Recommendations for the use of ESPs"

d. Does the contract with the external service providers foresee the possibility to involve the national DPA as the national supervisory authority[15] in the Member State's audits of the external service provider?
e. Does the contract provide for suspension or termination if the external service provider breaches the rules set out in the contract?
f. Does the contract contain a review clause?
g. How do you verify that the external service providers actually carry out the tasks specified in the contract on the basis of Article 43(6) of the Visa Code?

## X. Data subject rights (these questions should be addressed regarding the ESP)

*Specific legal provisions: Articles 37 and 38 VIS Regulation, and Annex X, A (h) Visa Code*

172. Where is general information on visa requirements and application forms available?
173. Where is the list of sub-processors/third parties working on your behalf available?
174. Right to information:
    a. How is this right provided to the data subject?
    b. Locally or centrally?
    c. Where is it possible to find information on the rights and freedoms?
    d. How is the right to information made concrete for the visa applicant (e.g., information on the website, brochure for visa applicants, form with information on VIS and how to exercise the rights);
        i. In which languages?
        ii. When is this information provided?
175. Right of access // Right to correction // Right to data deletion
    a. Locally or centrally?
    b. What is the procedure?
    c. Are third parties involved?
    d. Link with retention periods and cleaning up of files?
    e. Are third parties involved?
176. What information is provided to applicants who have received a visa refusal?
    a. In what form and when?
    b. In which languages can visa applicants receive this information?

[15] According to Article 41 of the VIS Regulation, and Article 43 (9) of the Visa code

# Questions to external provider(s) (subcontractors)

## Y. Procedures of the ESP

*Specific legal provisions: Article 43/44 Visa Code, Annex 10 Visa Code*

177. How is personal data handled/transferred between the external provider and the consulate/embassy?
178. What systems does the supplier use to collect personal data?
179. On average, how many visa applications per year does the ESP receive and manage on behalf of the Member State?
180. What are the figures for the last 3 years?
181. How long does it take on average to process the Visa application at this ESP?
182. What security measures are in place during the data collection and processing?
183. Clarify whether external personnel, other than ESP staff, have access to the ESP premises.
184. Please provide further information on:
    a. the organization of the ESP;
    b. the total number of staff employed on behalf of the Member State;
    c. the different functions and roles (which is related to the physical and technical identity and access rights);
    d. a list of the staff members who have access to the personal data of visa applicants vis the system application of the ESP
185. Are there any confidentiality clauses in place in the staff contract?
186. Are employees trained on how to protect and secure data? Provide documentation.
187. Are specific instructions and procedures on data protection (right of access, correction, data erasure etc.) provided to staff?
188. Are there any instructions/procedures/tools for checking the authenticity of documents? What is the procedure if there is any doubt about the authenticity of a document?
189. What happens to the personal data collected/processed on behalf of consular posts/embassies?
    a. Where is it stored?
    b. How long is it stored?
    c. How is it deleted?
    d. Does the provider have a procedure for handling this data?
190. Do you have a personal data breach procedure/policy in place?
    a. Do you provide training awareness to your staff on personal data breach management?
    b. Is there a mechanism to report data breaches to consular posts/embassies?

c. Were there any personal data breaches incidents regarding the personal data collected/processed on behalf of consular posts/embassies? If yes, what measures were taken?

# Abbreviations and acronyms

| | |
|---|---|
| CIP | Common inspection plan |
| CS-VIS | Central visa information system |
| DPO | Data protection Officer |
| EDPS | European Data Protection Supervisor |
| ESP | External service providers |
| eu-LISA | European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice |
| GDPR | General data protection regulation (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data) |
| ISO | International Organization for Standardization |
| MS | Member state |
| NS-VIS | National visa information system |
| SA | Supervisory authority |
| SCG | Supervision coordination group |
| SCHEVAL | Schengen Evaluation |
| SIRENE | Supplementary Information Request at the National Entries |
| VIS | Visa information system |

# Annex - Self-assessment questions for supervisory authorities

The purpose of this Annex is to provide elements that would allow supervisors to conduct a self-assessment.

*Specific legal provisions: Article 41 VIS Regulation*

1. Which national data protection supervisory authorities (SAs) are competent for the supervision of the VIS in order to ensure compliance with data protection requirements?
    a. If there are several SAs in charge of the data protection supervision of VIS, please specify and explain the distribution of tasks between the different authorities as well as their cooperation and coordination.
    b. Is the SA competent for supervising data protection in the VIS also competent to supervise data protection in all authorities having access to those databases (e.g. law enforcement authorities, immigration authorities)?
2. Does the SA have a supervision plan for VIS?
3. Has there been an audit of the VIS national instance by the SA in the last 4 years?
    a. When was the last audit?
    b. What was the purpose of the audit?
    c. What was the scope of the audit?
    d. What methodology was used?
    e. Was the VIS system accessed?
    f. What were the main findings and recommendations of the SA?
    g. Was there any follow-up to the results of the audit?
4. Has the SA carried out an audit of embassies/consulates?
5. Has the SA carried out an audit of external service providers?
6. Has the SA carried out an audit of authorities having access to the VIS in accordance with VIS Decision?
7. Has the SA performed any audit of other national authorities having access to the VIS (e.g. immigration offices)?
8. Does the SA website provide an English template for lodging a complaint concerning personal data processing in the national visa system?
9. Has the DPA received any complaints regarding restrictions on data subjects exercising their rights of access to, rectification, completion, and erasure of personal data, as provided for in Article 38 VIS Regulation?