Council of the European Union

Brussels, 25 November 2024
(OR. en)

15705/24

Interinstitutional File:
2024/0126(NLE)

LIMITE

SCH-EVAL 136
DATAPROTECT 319
COMIX 459

NOTE

From:	European Commission
To:	Delegations
No. prev. doc.:	10643/24
Subject:	Draft Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2021 evaluation of Italy on the application of the Schengen acquis in the field of data protection.

Delegations will find in annex a draft Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2021 evaluation of Italy on the application of the Schengen acquis in the field of data protection.

Changes compared to the previous document are marked **bold/underlined** and ~~strikethrough~~.

ANNEX

Draft

COUNCIL IMPLEMENTING DECISION

setting out a recommendation on addressing the deficiencies identified in the 2021 evaluation of Italy on the application of the Schengen *acquis* in the field of data protection

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen[1], and in particular Article 15(3) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) A Schengen evaluation in the field of personal data protection was carried out in respect of Italy in September 2021. Following the evaluation, a report covering the findings and assessments, listing best practices and deficiencies identified during the evaluation was adopted by Commission Implementing Decision C(2024)1910.

1 OJ L 295, 6.11.2013, p. 27.

(2) As good practices are seen in particular: the extensive security measures regarding the physical security for the National Schengen Information System (N.SIS) server; the comprehensive training provided for N.SIS and SIRENE Bureau staff members and end users, especially regarding the training and awareness raising efforts made by the Data Protection Officer (DPO) office; the extensive efforts of the DPO Office to enhance data protection and data security including for the N.SIS ; the regular inspections carried out by the Ministry of Foreign Affairs and International Cooperation (MFAIC) at embassies and consulates as well as the inspection at External Service Providers (ESPs) carried out by the embassies and consulates on the basis of a guidance document by the MFAIC; the posters at the airport and at the police station, which provide easy access to information about the SIS through QR-Codes in multiple languages; the information on the Schengen Information System (SIS) data subjects rights provided on the websites of the Polizia di Stato and the Data Protection Authority (DPA) as helpful and accessible; that the website of the Ministry of Interior (MoI) entails links to the homepage of the Polizia di Stato, which provides data subjects with an easy and fast way of exercising their rights; that the Polizia di Stato informs the data subjects if their data is not contained in SIS; the information on the Visa Information System (VIS) data subjects rights provided on the website of the DPA as helpful and accessible.

(3) Recommendations should be made on remedial actions to be taken by Italy in order to address deficiencies identified as part of the evaluation. In light of the importance of complying with the Schengen *acquis* on personal data protection and specifically on the supervision by the DPA and on the SIS and VIS training priority should be given to implementing recommendations 4 and 6 set out in this Decision.

(4) In accordance with Article 15(3) of Regulation (EU) No 1053/2013, the Council should transmit this Decision to the European Parliament and to the national Parliaments of the Member States.

(5) Council Regulation (EU) 2022/922[2] applies as of 1 October 2022. In accordance with Article 31(3) of that Regulation, the follow-up and monitoring activities of evaluation reports and recommendations, starting with the submission of the action plans, should be carried out in accordance with Regulation (EU) 2022/922.

(6) Within two months of the adoption of this Decision, Italy should, pursuant to Article 21(1) of Regulation (EU) 2022/922, establish an action plan to implement all recommendations and to remedy the deficiencies identified in the evaluation report. Italy should provide that action plan to the Commission and the Council.

---

2 Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis, and repealing Regulation (EU) N° 1053/2013, OJ L160 of 15.6.2022, p. 1.

RECOMMENDS that

Italy should:

Data Protection Authority

1. ensure that the DPA is formally involved in the budgetary procedure, in particular that it has formal influence on the proposal for its budget before the general budget proposal is sent to the Parliament for discussion and adoption.

2. ensure that the DPA is allocated sufficient staff in order to carry out the SIS and VIS supervision in a timely and effective manner.

3. carry out regular inspection of some end user authorities of the system such as operational police authorities, including regular checks and analysis of the log files in order for the DPA to fulfil its tasks of comprehensively monitoring the processing of personal data within the SIS.

4. finalise the pending audit of the data processing operations in N.SIS as soon as the COVID19 situation allows and ensure that the following audits are carried out within the prescribed term of four-year cycle.

5. ensure that also more end user authorities of the VIS system such as the police, border guards and immigration authorities are inspected on a regular basis in order for the DPA to fulfil its tasks of comprehensively monitoring the processing of personal data within the VIS.

6. ensure that the audits of the national visa system are carried out within the prescribed term of four-year cycle.

7. ensure that the VIS audits in addition to the auditing measures of the MFAIC also comprise the MoI as the other VIS controller.

Schengen Information System

8. ensure that the separate disaster recovery site in Bari becomes operational.

9. ensure that the backup copy of N.SIS log files is kept off-site, in another geographical location than Rome, not only in a systematic way but with a relevant short period of time between making of copies.

10. ensure that the operating systems at some work-stations such as the SIRENE Bureau and at the local police station at the Commissariato Trevi-Campo Marzio, are updated as soon as possible.

11. ensure that for monitoring SIS log files guidelines with criteria applicable to all monitoring staff are adopted and a software module for the actual analyses of SIS log files with an automatic warning system for unusual queries is implemented in order to identify misuse.

12. ensure a higher security standard in relation to the access to databases such as the SIS application using a two-factor authentication system.

13. ensure that the DPA and the MoI develop a common understanding or protocol concerning the criteria or threshold for notification of N.SIS data breaches to the DPA.

14. reassess and implement the group policy rules for automatic locks regarding computer systems in cases of inactivity at every workstation with access to the SIS.

15. **Establish a security and data protection policy and monitor the** ~~review legislation and~~ practice on keeping accommodation registration personal data in a police data base **to provide that, after all personal data are kept for the necessary checks in the initial period, regular review ensures that, within the maximum retention period,** ~~in order to keep them only as long as those~~ **personal** data ~~are~~ **remain stored in a police database only for as long as** necessary **and proportionate** for the purposes pursued **by Article 45 of the Schengen Convention**[3].

Visa Information System

16. establish a reasonable limit of failed login attempts, considering mistype errors, memory confusion, etc., on the basis of which the user should be blocked by the system when accessing the National Visa Information System (N-VIS).

17. implement additional measures to monitor the N.VIS access authorisations (in addition to N.VIS users being subject to a strict and regular revision of their access authorisations by the office they belong to), in order to ensure effectiveness and efficiency of the revision process e.g. automatic suspension of the access authorisation after a large and atypical period of time without any activity on the VIS system.

18. provide a higher security level by combining the badge reading with the insertion of a personal pin code, at the two RFID readers installed at the entrance of MFAIC Data Centre zone and at the Visa server room.

---

[3] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, (OJ L239, 22.09.2000).

19. apply the same policy already adopted for other equipment at the N.VIS server room also for the equipment stored in locked cabinets.

20. implement a proper security system, capable to provide room access authentication and event auditing and further provide the VIS system backup server room with a fire suppression system for electrical equipment like the one installed at the VIS server room.

21. implement a disaster recovery infrastructure on a different geographical location than the Farnesina building.

22. review the backup processes implemented at Embassies and Consulates, avoiding the usage of pen drives, or in case of using them, encrypt the stored information.

23. implement an automatic log control of I-VIS logs.

24. add a personal data protection module to the pre-posting in-house training course which is provided to staff dealing with visa issuing.

25. ensure the MFAIC assesses the criticalities of the local warning lists highlighted by the DPA, not only at a domestic level but also by liaising with the other consulates involved, and informs the DPA in due time about the measures that may be adopted to ensure full compliance with personal data protection requirements.

26. reinforce the office of the DPO of the MFAIC.

Public Awareness and Rights of Data Subjects

27. ensure that the information about SIS on the website of MoI is also comprehensible to non-Italian speakers.

28. ensure that model letters on the websites of the DPA concerning SIS are provided and the button on the relevant website "The new mechanism to exercise data protection rights" is made more visible.

29. change the standard response that "the data subject has no entry bans in the Schengen territory" (no. 6) which is considered as misleading in cases where no information about the alert is provided to the data subject for instance due to threats to public or national security.

30. ensure that the websites of the MFAIC and the MoI provide for a specific template for a VIS personal data access request relating to personal data processed within the VIS.

31. consider providing information on the VIS and the rights of data subjects' relating to processing of personal data within the VIS at border crossing points such as airports in the same way as is already done for the SIS for instance through posters, a QR code with link to more information, etc.

Done at Brussels,

For the Council
The President