Council of the European Union

Brussels, 24 September 2024
(OR. en)

13734/24

Interinstitutional File:
2024/0147(NLE)

SCH-EVAL 121
DATAPROTECT 281
COMIX 392

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12304/24
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2021 evaluation of Malta on the application of the Schengen acquis in the field of data protection

Delegations will find enclosed the Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2021 evaluation of Malta on the application of the Schengen acquis in the field of data protection, adopted by the Council on 24 September 2024.

In line with Article 15(3) of Council Regulation (EU) No 1053/2013 of 7 October 2013, this Recommendation will be forwarded to the European Parliament and national Parliaments.

ANNEX

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2021 evaluation of Malta 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 Malta in November 2021. Following the evaluation, a report containing the findings and assessments, listing best practices, areas of improvements and deficiencies identified during the evaluation was adopted by Commission Implementing Decision C(2024)2501.

(2) The following best practices were identified: close cooperation between the Malta data protection authority (IDPC) and the Malta Police Force data protection officer (DPO). The Malta Police Force DPO consults the IDPC regularly about the data protection requirements of the second-generation Schengen Information System (SIS II) and the self-auditing mechanisms of the Ministry of Foreign and European Affairs (hosting the national visa information system, N.VIS).

[1] OJ L 295, 6.11.2013, p. 27.

(3) Recommendations should be made on remedial actions to be taken by Malta in order to address deficiencies and areas of improvement identified during the evaluation. In light of the importance of complying with the Schengen *acquis* on personal data protection and specifically on the supervision by the IDPC and on the Schengen Information System (SIS) and Visa Information System (VIS) priority should be given to implementing recommendations 1, 2, 3, 10,15 and 25 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, Malta should, pursuant to Article 21(1) of Regulation (EU) No 2022/922, establish an action plan to implement all recommendations and to remedy the deficiencies identified in the evaluation report. Malta should provide that action plan to the Commission and the Council.

RECOMMENDS

that Malta should:

Legislation

1. ensure the implementation of the new SIS and VIS rules takes place as soon as possible.

Data Protection Authority

2. increase the budget of the IDPC so that it has sufficient human and technical resources in order to audit large-scale databases, such as SIS II and VIS, and to help to ensure access to specialised trainings.

3. ensure that the audits of the national VIS and SIS II are carried out within the prescribed term of four-year cycle, and are comprehensive, including the audits of in-direct logs.

4. provide for a formal arrangement between the IDPC and the police DPO to ensure a prompt response to any data breach.

[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.

Schengen Information System

5. ensure the separation of the tasks of the International Relations Unit and that its premises have an appropriate separation of the access controls between the different sectoral sub-units (Europol, Interpol, SIS II) sharing those offices.

6. develop and implement a comprehensive security plan in accordance with the requirements of Article 10(1)(a) of SIS II Regulation[3] and SIS II Council Decision[4] and the new SIS II *acquis*.

7. ensure that access to SIS II and SIRENE applications includes robust user access control, including the implementation of a two-factor authentication system.

8. ensure that access to SIS II and SIRENE systems can take place only via secure and up-to date systems.

9. ensure that the Malta Police Force develops self-monitoring policies, including security elements, independently of the compliance audits developed by the DPO or the data protection authority, to ensure full compliance with Article 10(1)(k) of SIS II Regulation and SIS Council Decision.

10. improve self-monitoring of N.SIS by checking logs proactively and on a regular basis, including by using automatic log control.

11. update search function of the record system in line with data protection by design and by default, in particular to allow for retrieving and displaying only a limited number of search results.

12. implement automated technical means to detect and notify the head of SIRENE Office, in case of a detection of an abnormal activity in the logs implemented.

13. ensure that the Malta Police Force conducts a data protection impact assessment to identify the risks to data subject and consults the IDPC on the results and implement an action plan on how to mitigate the detected risks.

Visa Information System

14. carry out regular checks on the validity of user authorisation and access rights.

15. improve self-monitoring of N.VIS by checking logs proactively, that is on a regular basis, including by using automatic log control.

3 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4–23

4 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p. 63–84

16. ensure audit of consular posts regularly.

17. ensure that the DPO position of Identity Malta is fully independent and its tasks and duties do not result in a conflict of interest.

18. ensure that the DPO position of MFEA does not result in conflict of interest, in particular by identifying the positions which would be incompatible with the function of MFEA DPO, and drawing up internal rules to ensure that other tasks and duties of the DPO do not result in a conflict of interests.

Public awareness and rights of data subjects

19. provide for a secure channel for the transmission of personal data to the Malta Police Force and other authorities involved in operating the SIS.

20. provide for the possibility for data subjects to submit a data subject right request at a police station.

21. ensure that the application forms relating to the exercise of data subjects' rights are made readily available in all the police stations.

22. ensure that the information provided on the MFEA website, in particular links to the IDPC Schengen leaflet, the retention policy for visa applications, and the VIS factsheet, refer to the currently applicable legislation.

23. ensure that the IDPC contact details, which are provided in the MFEA Subject Access Request Policy on its website, are accurate.

24. ensure that data subjects are informed about the risks of submitting copies of ID documents and sensitive information through a non-secured channel (unencrypted emailing system) to the MFEA and the Identity Malta and provide a secure channel for submitting such documents.

25. ensure that the website of the Identity Malta provides adequate information on VIS, in particular by including explicit reference to the rights of data subjects relating to their visa applications and provide information regarding their exercise, even if it is not possible to apply for a visa online, through the website.

26. ensure that the information about personal data processing in SIS II and VIS by IDPC is also provided in Maltese.

Done at Brussels,

For the Council
The President