Council of the European Union

Brussels, 24 May 2024
(OR. en)

10357/24

Interinstitutional File: 2024/0081(NLE)

SCH-EVAL 78
DATAPROTECT 221
COMIX 249

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	9411/24
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2022 evaluation of **Spain** 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 2022 evaluation of Spain on the application of the Schengen acquis in the field of data protection, adopted by the Council at its meeting held on 24 May 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 2022 evaluation of Spain 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 Spain in March 2022. 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)650.

1 OJ L 295, 6.11.2013, p. 27.

(2) As good practices are seen in particular: the very active involvement of the Spanish Data Protection Authority (AEPD) in international cooperation, in particular the regular participation in Schengen Evaluations; the AEPD's detailed planning with a four year rhythm for the evaluation of the authorities managing and using the Schengen Information System (SIS) and the Visa Information System (VIS); the extensive efforts of the SIRENE Bureau staff to provide data protection training to the staff of SIS end user authorities; the comprehensive, extensive and multi-layered self-auditing by the Ministry of Foreign Affairs, European Union and Cooperation (MFAC); the comprehensive data protection training provided by the MFAC to consular staff; the strong involvement of the MFAC's data protection officer (DPO) in many data protection aspect of the visa issuing procedure; that the AEPD provides on its website detailed information about the SIS-system and the VIS-system and related data subjects' rights including standard templates for exercising those rights in both Spanish and English.

(3) Recommendations should be made on remedial actions to be taken by Spain to address deficiencies identified as part of the evaluation. Considering the importance of complying with the Schengen *acquis*, priority should be given to implementing recommendations 4, 5, 6, 12 and 19 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, Spain 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. Spain 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

Spain should:

Data Protection Authority

1. ensure that during the budgetary procedure the Spanish Data Protection Authority (AEPD) can exercise its right to draw up and approve its budget as well as to send it to the Government so that it may be independently integrated into the General State Budget as laid down in Article 46 (1) LO 3/2018[3];
2. ensure that the DPA has adequate resources to fulfil the tasks entrusted to it under the SIS and VIS acquis;
3. ensure that the AEPD develops a systematic approach to the use of log files in all SIS inspections for monitoring the lawfulness of the processing of personal data in SIS;
4. ensure that the AEPD finalises the second N.SIS audit as soon as possible and carries out the future N.SIS audits within a four-year cycle;
5. ensure that the AEPD finalises the second N.VIS audit as soon as possible and carries out the future N.VIS audits within a four-year cycle;

Schengen Information System

6. review legislation and practice on keeping accommodation registration personal data in a police data base in order to keep them only for as long those data are necessary for the purposes pursued;
7. ensure that the N.SIS data recovery centre is put in place and becomes operational as soon as possible;
8. ensure that the Spanish authorities quickly finalise the setting up of the N.SIS back-up site;
9. ensure that the Spanish authorities carry out a security audit of the N.SIS;

3 Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LO 3/2018)

10. ensure that the Spanish authorities check the SIS logs proactively (thus not only incident related) including by using automatic log control;

11. ensure that the Spanish authorities regularly check the validity of N.SIS user authorisations;

12. ensure that retention period for N.SIS logs of the activities of the SIRENE Bureau staff are brought in line with the SIS acquis, thus that records will be deleted at the latest three years after their creation and may be kept longer if they are required for monitoring purposes that are already underway;

Visa Information System

13. correct the Schengen visa application form in such a way that the MFAC is described as the controller of VIS-data;

14. establish clear requirements and a procedure (applicable to all border posts) for the retention and deletion of personal data contained in visa application files;

15. ensure that the MFAC carries out regular checks on the validity of user authorisations and access rights;

16. ensure that the MFAC makes proactive checks of logs in order to detect unlawful processing of data including with an automatic log control tool, possibly by extending and further developing the pilot project executed by ESDEFE,

17. ensure that the Police carries out pro-active checks of ADEXTTRA logs including with an automatic log control tool to detect unlawful processing of data;

18. ensure that the Police staff at Madrid Airport receives sufficient training on data protection concerning the visa issuing procedure including VIS;

19. ensure that deletion is carried out according to Article 25 VIS-Regulation when the person has acquired the nationality of a Member State;

Public awareness and rights of data subjects

20. ensure that the information on data protection on the MoI's website is easier to find, that it is provided also in another language e.g. English and contains information about data subjects' rights under SIS including on the procedure to exercise the rights to rectification and erasure (including standard forms for those purposes); that the MoI's website has a direct link to the AEPD website;

21. ensure that the national police provides the same standard form for the exercising the right of access to SIS data as the MoI and the AEPD;

22. ensure that the replies to SIS access requests contain more accessible information about the complaint mechanism;

23. ensure that the standard forms provided by the MoI and AEPD contain also information on the right of data subjects to lodge a complaint if they consider that the processing of personal data related to them infringes the GDPR, the LED and national data protection law; ensure that the replies to data subjects contain information about the right to judicial remedies against the decision of the MoI;

24. ensure that at the airport(s) information about data processing and rights in the context of SIS is made easily accessible;

25. ensure that the MoI in its role as controller of N.SIS deals with requests of data subjects for rectification or erase and organises the contact with the authority which has issued the alert in SIS; the reaction of the data subject has to be provided by the controller;

26. ensure that the templates and replies to VIS data subjects' requests contain information about the right to challenge the decision before national courts;

27. ensure that information is proactively provided to data subjects during their application for a visa at the borders about the processing of their personal data in VIS and the related data subjects' rights; further a standard template for exercising those data subjects' rights should be provided;

28. ensure that the websites of the MoI and the Police provide information about the exercise of VIS data subjects' rights.

Done at Brussels,

For the Council
The President