Council of the
European Union

Brussels, 24 September 2024
(OR. en)

13736/24

Interinstitutional File:
2024/0018(NLE)

SCH-EVAL 122
DATAPROTECT 282
COMIX 393

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12299/24
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2022 evaluation of Sweden 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 Sweden 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 2022 evaluation of Sweden 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 Sweden in June 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)340.

(2) As good practices are seen in particular: strengthening the office of the data protection officers within the Swedish Police Authority and incorporating several data protection experts working alongside the data protection officers; implementation of the new SIEM tool, which significantly improves the detection of anomalies and potential misuse of systems, including the Schengen Information System (SIS); the Swedish Migration Agency's log system solution and implementation of software "Splunk" in carrying out checks of logs of National Visa Information System (N.VIS); and clear information on the website of the Swedish Authority for Privacy Protection on the SIS and the Visa Information System (VIS), including links to the standard forms for exercising data subjects' rights, provided on the websites of the Swedish Police Authority and the Swedish Migration Agency.

1 OJ L 295, 6.11.2013, p. 27.

(3) Recommendations should be made on remedial actions to be taken by Sweden 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 1, 2, 4 and 7 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, Sweden 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. Sweden should provide that action plan to the Commission and the Council.

RECOMMENDS

that Sweden should:

Data Protection Authority

1. ensure that the employment conditions of the Director-General of the Swedish Authority for Privacy Protection (*Integritetsskyddsmyndigheten*) meet the requirements to ensure the independence of the Authority, in conformity with Article 53(4) of Regulation (EU) 2016/679[3] and Article 43(4) of Directive (EU) 2016/680[4], as concerns the possibility of repositioning the Director-General;

2. review the legislation to ensure that data subjects can exercise their right to an effective judicial remedy also in the cases where the Swedish Authority for Privacy Protection has decided that a data subject's complaint does not give rise to further investigation or supervisory action and in the cases of delay or inactivity of the authority, as required in Article 78 of Regulation (EU) 2016/679 and Article 53 of Directive (EU) 2016/680;

---

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.

3 OJ L 119, 4.5.2016, p. 1-88.

4 OJ L 119, 4.5.2016, p. 89-131.

3. ensure that, in addition to the police, the Swedish Authority for Privacy Protection inspects on a regular basis some other end-users of the National Schengen Information System (N.SIS), for instance the VIS authorities, including checks of SIS alerts on the basis of log-file analysis;

4. ensure that the Swedish Authority for Privacy Protection finalises the pending N.SIS audit as soon as possible and carries out the follow-up audits of the N.SIS within the four-year cycle, as required in Article 44(2) of Regulation (EC) No 1987/2006[5] and Article 60(2) of Council Decision 2007/533/JHA[6];

5. ensure that the Swedish Authority for Privacy Protection inspects on a regular basis consular posts, including external service providers, and also other end users of the N.VIS, for instance law enforcement authorities, including checks of VIS files also on the basis of log-file analysis;

6. ensure that the Swedish Authority for Privacy Protection audits also the visa issuing procedure and related processing of personal data in the N.VIS by the police at external border-crossing points;

7. ensure that the Swedish Authority for Privacy Protection carries out follow-up audits of the N.VIS within the four-year cycle, as required in Article 41(2) of Regulation (EU) No 767/2008[7] and Article 8(6) of Council Decision 2008/633/JHA[8];

Schengen Information System

8. ensure that the N.SIS data recovery centre is put in place and becomes operational as soon as possible;

9. ensure that the reason or purpose for individual consultation of the N.SIS is required to be provided by the user and recorded in the SIS logs;

10. ensure that the Swedish Police Authority introduces a policy for its computers and databases requiring the renewal of the password (PIN code) regularly;

11. ensure that the guidelines of the Swedish Police Authority on the handling of personal data breaches are also directed and applied, for instance regarding the notification process in relation to the Swedish Authority for Privacy Protection, to the potential misuse of personal data by staff;

---

5 OJ L 381, 28.12.2006, p. 4-23.
6 OJ L 205, 7.8.2007, p. 63-84.
7 OJ L 218, 13.8.2008, p. 60-81.
8 OJ L 218, 13.8.2008, p. 129-136.

12. ensure that the Swedish Police Authority carries out and documents regular testing of recovery from the N.SIS backup;

Visa Information System

13. ensure that a disaster recovery site (secondary site) for N.VIS is established at a different distant location as soon as possible;

14. ensure that the Swedish Migration Agency intensifies the general training on data protection, makes it mandatory for all of its staff and includes a specific data protection part also into the pre-posting training for consular staff;

15. ensure that the relationship between the Swedish Migration Agency and the Swedish Police Authority for issuing visas at the border is clarified and laid down formally, for instance in an agreement;

16. ensure that the Swedish Migration Agency introduces a policy for its computers and databases that requires the renewal of the password (PIN code) regularly;

17. ensure that the Swedish Migration Agency clarifies with the Swedish Authority for Privacy Protection what type of personal data breaches fall under the notification obligation;

18. ensure that the Swedish Migration Agency and the Swedish Police Authority finalise as soon as possible the technical solution to integrate border police visa issuing with N.VIS to enable the Swedish Police Authority to register those visa files also in the N.VIS;

Public awareness and rights of data subjects

19. ensure that the Swedish Authority for Privacy Protection provides information on its website on the SIS and the VIS in a way that is as easily accessible for non-Swedish speakers as for Swedish speakers;

20. ensure the Swedish Police Authority provides on its website a standard form for data subjects' requests to erase or rectify their personal data;

21. ensure that the Swedish Police Authority provides in its model replies information about data subject's right to submit a complaint to the Swedish Authority for Privacy Protection;

22. ensure that the Swedish Authority for Privacy Protection and local police districts, including border-crossing points at airports, have available printed information material on the SIS and data subjects' rights addressed to the public;

23. ensure that the Swedish Migration Agency provides information on its website on the VIS and data subjects' rights in an easily accessible way;

24. ensure that the internal guidance of the Swedish Migration Agency on the maintenance of the VIS is fully line with Article 12(5) of Regulation (EU) 2016/679 regarding the conditions under which the data controller may refuse to act on the data subject's request;

25. ensure that the Swedish Migration Agency's replies to data subjects' requests provide information on all remedies available to data subjects at national level;

26. ensure that the websites of Sweden's consulates and embassies as well as the websites of the external service providers provide information on the VIS and adequate information on data subjects' rights;

27. ensure that Swedish Authority for Privacy Protection and border-crossing points have available printed information material on the VIS and data subjects' rights addressed to the public;

28. ensure that, in addition to the information included in the application form for an emergency visa, information on data subjects' rights and remedies in the context of VIS is provided without data subject's specific request during the emergency visa-issuing procedure at external borders, for instance at Stockholm Arlanda airport.

Done at Brussels,

For the Council
The President