Council of the European Union

Brussels, 8 March 2019
(OR. en)

7282/19

Interinstitutional File:
2019/0032(NLE)

SCH-EVAL 51
DATAPROTECT 85
COMIX 149

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	7 March 2019
To:	Delegations
No. prev. doc.:	6393/19
Subject:	Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2018 evaluation of **Finland** on the application of the Schengen acquis in the field of **data protection**

Delegations will find in the annex the Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2018 evaluation of Finland on the application of the Schengen *acquis* in the field of data protection, adopted by the Council at its meeting held on 7 March 2019.

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 2018 evaluation of Finland 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 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The purpose of this Decision is to recommend to Finland remedial actions to address the deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2018. 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(2019)290.

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

(2) As good practice are seen amongst others the outstanding security and contingency measures at the data centre in Rovaniemi, multi-layered authentication requirements imposed on police officers, the dedicated data protection training provided to Police staff and the fact that the Police replies to all data subject requests, no matter in which language they were made.

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the Schengen Information System II (SIS II), priority should be given to recommendations 16 and 21.

(4) In light of the importance of complying with the Schengen acquis on data protection in relation to the Visa Information System (VIS), priority should be given to recommendations 5 to 10.

(5) Furthermore, in order to ensure legal certainty, it is essential to swiftly adopt national laws implementing the General Data Protection Regulation (EU) 2016/679 and transposing the Data Protection Directive (EU) 2016/680, including the founding act of the Data Protection Ombudsman that ensures its complete independence and strengthens its supervisory activities.

(6) This Decision should be transmitted to the European Parliament and to the parliaments of the Member States. Within three months of its adoption, Finland should, pursuant to Article 16 (1) of Regulation (EU) No 1053/2013, establish an action plan listing all recommendations to remedy any deficiencies identified in the evaluation report and provide that action plan to the Commission and the Council,

RECOMMENDS:

that Finland should

Data protection supervisory authority

1. ensure the complete independence of the Data Protection Ombudsman (DPA) by providing that its Head of Office is appointed by the Ombudsman her/himself, instead of by the Ministry of Justice;

2. ensure that the supervisory activities of the DPA in relation to the SIS II include regular controls of SIS II alerts;

3. ensure that the supervisory activities of the DPA in relation to the VIS include regular inspections of Consular Posts;

4. ensure that the DPA's multi-annual inspection plan includes other inspection activities than the mandatory audits of SIS II and VIS;

Visa Information System

5. ensure that the external service provider can only send visa applicant data through secure VPN and in encrypted form;

6. ensure that visa applicant data is not retained on servers of the external service provider;

7. ensure that the external service provider creates alternative means for transmission of applicant data from China and Russia to the United Kingdom;

8. sign the data protection agreement with the external service provider and clarify the respective responsibilities of the Ministry of Foreign Affairs (MFA) as a data controller in relation to VIS and the external service provider as the data processor;

9. ensure that log files are kept by the MFA and analysed regularly for data protection self-monitoring and set up procedures of self-auditing/self-monitoring of personal data processing in SUVI on a regular basis;

10. ensure that the MFA exercises effective control over the national Visa Information System;

11. set up a recovery site for SUVI in a different location from the main SUVI server;

12. ensure that the MFA keeps the repository of ELVIS users;

13. ensure that the data protection agreement between the MFA and Tieto meets the requirements on controller-processor agreements as provided by the General Data Protection Regulation (EU) 2016/679;

14. ensure that the MFA develops training for its staff and the employees of consulates or embassies that is dedicated specifically to personal data protection issues related to VIS;

15. ensure that the data protection officer of the MFA is involved in processing of personal data, case handling and training of the staff;

Schengen Information System

16. ensure that the Police carries out self-auditing on a regular basis, in particular self-monitoring of logs;

17. clearly define the role of the data protection officer and ensure the involvement of the data protection officer in the data protection work, as well as ensure the improvement in the relationship between different data protection entities of the Police (the data protection officer, data protection group, data protection coordinators and cooperation group for data protection);

18. ensure an integrated system that displays both national and international alerts simultaneously to the end user in case of a query;

19. ensure that photographs, fingerprints, and other mandatory SIS II data are integrated in the SIS II alerts in a secure way;

20. clarify the division of tasks for IT security within the Police;

21. generate national SIS II logs at a central level and ensure that the justification for the query can be established from the log;

Rights of data subjects and awareness raising

22. ensure alternative options for effective exercise of the data subject rights of access, rectification and erasure of SIS II and VIS data;

23. reduce the amount of the fee for every second and following access request within 12 months, in order for the data subjects to have the effective right of access to their SIS II data;

24. provide an answer to the data subjects when exercising their indirect access within a period that is compliant with the Schengen acquis;

25. ensure the availability of a template letter on the exercise of the right of rectification and erasure to SIS II and VIS data;

26. ensure the involvement of the respective data protection officers when handling requests from the data subjects exercising their rights in relation to SIS II and VIS data;

27. ensure the existence of centralised record regarding the data subject requests to SIS II data;

28. provide the DPA with the statistics concerning the exercise of data subject rights related to SIS II on an annual basis;

29. provide clear information to data subjects about the exercise of data subject rights indirectly with the DPA, when that right is limited in accordance with law;

30. provide information regarding the rights of the data subjects in relation to SIS II and VIS and more general information about data protection on the DPA's website, information regarding the rights of the data subjects in relation to VIS on the MFA's website and more easily accessible general information on data protection on the MFA's website, as well as on the websites of the embassies and consular posts.

Done at Brussels,

For the Council
The President