Council of the European Union

Brussels, 26 November 2018
(OR. en)

14763/18

Interinstitutional File: 2018/0338(NLE)

SCH-EVAL 228
DATAPROTECT 258
COMIX 648

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	26 November 2018
To:	Delegations
No. prev. doc.:	14114/18
Subject:	Council implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2017 evaluation of **Norway** 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 2017 evaluation of Norway on the application of the Schengen *acquis* in the field of data protection, adopted by the Council at its meeting held on 26 November 2018.

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 2017 evaluation of Norway 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 Norway remedial actions to address the deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2017. 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(2018) 4145.

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

(2) As good practice are seen amongst others that there is well developed training for NORVIS end users; that the Ministry of Foreign Affairs (hereafter MFA) has a comprehensive set of procedures, including the use of established check-lists, for monitoring the consular posts (hereafter CPs) and informing the CPs on practices to monitor the External Service Providers (ESPs); the extensive efforts of the National Criminal Investigation Service (hereafter NCIS) and the Police Districts as regards the training and awareness raising for their staff including on data protection issues; that the six Data Protection Officers (hereafter DPO's) at the NCIS have the lead on all legal and practical aspects of data protection for the NCIS and do play a very active role in the organisation; the similar commitment and proactive promotion of high level of data protection by the DPOs of the Police Districts.

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the Schengen Information System II and the Visa Information System, , priority should be given to implementing recommendations 8, 22, 27, 28 and 29 below.

(4) This Decision should be transmitted to the European Parliament and to the parliaments of the Member States. Within three months of its adoption, Norway 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 Norway should

Data Protection Supervisory Authority

1. in order to better ensure the complete independence of the Norwegian Data Protection Authority (hereafter DPA) amend the terms of the *'Instructions on Economy and Operations'* and the *'Grant Letter'* in such a way that they could not result in a risk of direct or indirect influence of the Government on the DPA which could endanger the independence of the DPA;

2. in order to better ensure the complete independence of the DPA, organise the informal meetings of the Commissioner of the DPA with the Ministry of Local Government and Modernisation (hereafter the Ministry) in such a way that it could not result in a risk of direct or indirect influence of the Government on the DPA which could endanger the independence of the DPA;

3. abolish all those elements of the subordinate position of the DPA to the King and the Ministry which could result in a risk of direct or indirect influence by the Government on the DPA and thus could endanger the DPA's independence;

4. in order to better ensure the complete independence of the DPA reform the budgetary procedure in such a way that the DPA has a real influence on the proposal for its budget before the general budget proposal is sent to the Parliament for discussion and adoption as well that the budgetary proposal of the DPA will be made known to the Parliament;

5. strengthen the powers of the DPA by giving it an effective way of enforcing its decisions with regards to unlawful processing of Schengen Information System II (hereafter SIS II) personal data;

6. ensure that the DPA monitors the lawfulness of the processing of SIS II personal data including the analysis of log-files on a more regular basis;

7 ensure that the DPA monitors the lawfulness of the processing of Visa Information System (hereafter VIS) personal data including the analysis of log-files on a more regular basis;

8. ensure that, at least every four years, audits of data processing operations in the national system of VIS will be carried out by the DPA. As the deadline for the first audit (October 2015) has not been met, action should be undertaken to fulfil this obligation as soon as possible;

Rights of Data Subjects

9. provide clear information on the relevant websites (in particular of the DPA and the Norwegian Police) about the two possibilities to exercise SIS II data subjects rights: Data subject can either submit a request to NCIS (with the possibility to lodge an appeal to the Police Directorate which takes a decision following an opinion of the DPA) or data subject can submit a request to the DPA;

10. abolish the obligation of data subjects to always provide a notarised copy of the document proving their identity except in situations where there are reasons for suspicion about the identity of the data subject;

11. provide information on the website of the Norwegian Police about the deadline for a reply to SIS II data subjects' requests and about the possibility to lodge an appeal to the Police Directorate and where to send such an appeal;

12. provide model letters for the exercise of VIS data subjects' rights on the websites of the DPA, the MFA and the CPs;

13. provide information on the website of the DPA about the possibility to contact the DPA directly regarding VIS issues, including making a complaint about VIS related data subjects' rights;

Visa Information System

14. ensure that the contract between the Norwegian Directorate of Immigration (hereafter UDI) and Sopra Steria (for operating and maintenance of the IT-infrastructure) contains specific deliverables for Sopra Steria to carry out routine actions for the maintenance of the system and that the UDI should ensure they have more control over all maintenance actions by Sopra Steria;

15. improve the physical security of the NORVIS server rooms by establishing a comprehensive set of criteria to ensure that Sopra Steria has sufficient control over the external IT supply and maintenance company, in particular in relation to security and access to the server rack;

16. consider setting up a NORVIS recovery site at a different location;

17. ensure that the UDI establishes a procedure for regular and proactive checking of the NORVIS log files, including administrator logs;

18. ensure that in respect of the requirement under Article 34 of the VIS Regulation for the deletion of log files (one year after the retention period of the data entered into the VIS has expired) a system (either automated or manual) should be put in place to ensure the logs are deleted on a regular basis;

19. ensures that the UDI considers to review the location for keeping backup tapes and ensures that the location is at an adequate distance from the datacentres and that there is regular testing of restoring the system;

20. ensures that further specific training for IT staff within the UDI is provided for them to be better informed for monitoring the system and actions of outsource companies;

21. ensure that the UDI prepares a more structured and comprehensive procedure for monitoring administration access to the NORVIS servers, regular pro-active log checks, inspections of the data centres and generally more active oversight on the activities of the IT management companies;

22. ensure that in view of Article 32 of the VIS Regulation the UDI reviews its actions and establishes effective procedures for logging activity in connection with access to the NORVIS system; the UDI should put in place an effective system to ensure Data Base Administrator/administrator actions are logged to enable UDI to monitor and have oversight of such activities;

Schengen Information System

23. ensure that the NCIS puts technical measures in place in order to prevent the use of personal USB sticks in SIRENE workstations;

24. ensure that the NCIS puts technical measures in place in order to register the documents printed from a SIRENE workstation;

25. ensure that the Norwegian police creates profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search data in the SIS II (as required by Article 10 (1) g of the SIS II Regulation and Article 10 (1) g of the SIS II Council Decision). In particular it must be ensured, that in addition to the SIRENE staff, access to SIS II is only granted to those police staff who for their work need to carry out police checks;

26. ensure that one SIS II data centre will be better secured, and that the process of establishing a new and more secure data centre in Q4 of 2019 will be accelerated**;**

27. ensure that in line with Article 38 (2) of the SIS II Regulation deleted foreign files where no hits have been made should be deleted one year after deletion of the related alert in the SIS II;

28. ensure that in line with Article 12 (4) of the SIS II Regulation and Article 12 (4) of the SIS Council Decision SIS II records are deleted at the earliest one year and at the latest three years after their creation;

29. ensure that the logs about all messages sent and received via the Schengen formidling (creation, update or deletion of Norwegian alerts) are deleted in line with the requirements of Article 12 (4) of the SIS II Regulation and Article 12 (4) of the SIS Council Decision SIS II;

Public awareness

30. ensure that the information on the website of the Norwegian Police on SIS II, the data subjects' rights and the responsibility of the DPA will be easier to find;

31. consider whether the DPA and the Norwegian Police authorities will provide printed information on the SIS II and on the related data subjects' rights addressed to the public;

32. ensure that comprehensive information addressed to the public with regard to the processing of personal data in VIS and the related data subjects' rights is made available on the websites of the DPA, MFA and consular posts;

33. consider whether the DPA and CPs will provide printed information addressed to the public on the VIS and the related data subjects' rights.

Done at Brussels,

For the Council
The President