Council of the European Union

Brussels, 8 March 2019
(OR. en)

7278/19

Interinstitutional File: 2019/0015(NLE)

SCH-EVAL 49
DATAPROTECT 82
COMIX 146

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	6391/19
Subject:	Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2017 evaluation of **Spain** 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 Spain 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 2017 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 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The purpose of this Decision is to recommend to Spain 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(2019)280.

(2) As good practice are seen the extensive activities of the Ministry of Foreign Affairs and Cooperation ('MFAC') in relation to the supervision of the consulates and of the external service provider, including on data security and data protection issues, as well as self-auditing activities performed by MFAC.

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

(3) In light of the importance of complying with the Schengen acquis on personal data protection in relation to SIS II and VIS, priority should be given to implementing recommendation(s) 20-22 , 28, 29 and 34 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, Spain 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 Spain should

Data Protection Supervisory Authority

1. in order to better ensure the complete independence of the Agencia Española de Protección de Datos ('AEPD'), ensure that the AEPD is in a position to defend its proposal for budget before Parliament or before such proposal is sent to the Parliament for discussion and adoption;

2. ensure that the AEPD monitors the lawfulness of the processing of the SIS II and VIS personal data on a frequent basis;

3. as regards supervision of SIS II, ensure that the scope of the audit by the competent Data Protection Authorities is extended to also include the audit of regional users of SIS II, finalise the on-going audit as soon as possible and ensure that such comprehensive audits will be carried out by competent Data Protection Authorities at least every four years;

4. as regards supervision of VIS, ensure that audits of data processing operations in the national system of VIS will be carried out by the AEPD at least every four years;

5. ensure that the follow up of inspections carried out by the competent Data Protection Authorities in relation to both SIS II and VIS is strengthened by either stipulating a specific deadline for implementing the recommendations, or by requesting the controller to inform the competent Data Protection Authorities about the implementation of the recommendations within a prescribed time frame;

6. ensure the AEPD finalises the procedure concerning the adoption of the reports following the inspections relating to the processing of the personal data within SIS II and VIS without delay;

Rights of Data Subjects- SIS II

7. ensure that the SIS II data controller provides easily accessible information on its website about the procedure to exercise data subjects' rights as well as standard forms for the same purpose. As a corollary, the controller's website should have a direct link to the AEPD website;

8. ensure that in reply to the requests of the data subjects, the SIRENE office provides information about complaint mechanisms;

9. provide the data subjects with the secure means of the electronic transmission of their requests and supporting documentation (and in particular the secure means of providing copies of the identification documents);

10. establish a written internal procedure on how to deal with the requests for the exercise of data subjects' rights in SIS II to ensure business continuity for treating such requests;

11. encourage the AEPD to publish the standard form for the exercise of the data subjects' rights in SIS II in other languages such as English and French in a way that is readily accessible for the data subjects and to add a link on the AEPD's website to the SIS II data controller's website;

Rights of Data Subjects - VIS

12. encourage the AEPD to publish the standard form for the exercise of the data subjects' rights in VIS, including in other languages such as English and French, in a way that is readily accessible for the data subjects;

13. ensure that the Ministry of Foreign Affairs and Cooperation ('MFAC') provides easily accessible on its website a standard form for exercise of the data subjects' rights, including in other languages (such as English and French). As a corollary, the controller's website should have a direct link to the AEPD website;

14. ensure that in reply to the requests of the data subjects MFAC provides them with information about complaint mechanisms;

15. for visas issued by the National Police at the borders, ensure that the National Police provides easily accessible information on its website about the procedure to exercise the data subjects' rights as well as standard forms for the same purpose. As a corollary, the National Police website should have a direct link to the AEPD website;

16. for visas issued by the National Police at the borders, establish a written internal procedure on how to deal with the requests for the exercise of data subject's rights in VIS to ensure business continuity for treating such requests;

17. ensure that data subjects are provided with clear information as regards the identity of the data controller for processing of their personal data in the framework of issuing Schengen visas;

Visa Information System

18. clarify the situation concerning the controllership of the processing of personal data in N.VIS (encompassing the applications used both by MFAC and by National Police for visas issued at the borders) in particular by clarifying the role of the National Police and by clarifying the allocation of responsibilities related to processing of personal data between National Police and MFAC;

19. provide for a formalised procedure that allows verification of SIS II hits in the course of the visa procedure;

20. ensure all N.VIS users' passwords are encrypted;

21. ensure that data on N.VIS server and backup tapes are encrypted;

22. ensure high level of the physical security of VIS server room at all times, in particular by proper maintenance and reparation of security measures for access to the server room;

23. fully implement Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences and ensure that logs for access to N.VIS data respect the requirements established therein, in particular by ensuring that logs of such access indicate the particular individual users requesting access to VIS data, the specific reason for access and contain the national file reference.

24. ensure that data in N. VIS are kept for no longer than five years, in line with Article 23 of Regulation (EC) 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation);

25. ensure that logs of the operations related to VIS data in all applications relevant for processing the VIS data (and in particular SIVICO, AVANCE and ADEXTTRA applications) are stored for no longer than one year after the retention period referred to in Article 23(1) of the VIS Regulation has expired, in line with periods defined in Article 34 (2) of VIS Regulation and Article 16 of the VIS Council Decision. For access logs to VIS, ensure that they are kept for the period of one year after the retention period referred to in Article 23(1) of the VIS Regulation has expired;

26. ensure that ESP deletes personal data of applicants it stores on its systems in line with deadlines of Annex X, part A, point (d), of the Visa Code, requiring such data are deleted immediately after their transmission to the consulate;

27. ensure that MFAC and National Police check the log files of all applications involved in processing of VIS data by MFAC and in Adexttra on a regular basis in order to ensure the data protection monitoring;

Schengen Information System II

28. provide for the full backup site with high priority, and ensure the backup tapes are stored separately as a matter of urgency;

29. provide for additional protection measures (i.e. two factor authentication) for the access to user profiles with far reaching access or editing rights to N.SIS II data (SIRENE users and administrators);

30. strengthen the access control to the SIRENE office by ensuring that its premises are accessible only for the authorised police functionaries;

31. ensure a regular and continuous training of the end users with regard to the data protection in the SIS II;

32. implement a user management that allows for an effective self-monitoring on the basis of central logs by the N.SIS II data controller without the need to consult logs at user authorities;

33. ensure that the N.SIS data controller provides for the comprehensive security policy with respect of the SIS II data which also cover the IT security measures for access of N.SIS II data including control and self-monitoring measures or training authorities accessing SIS.II (user authorities). Spain is encouraged to clarify the responsibilities between the parties involved in processing of N.SIS II data, that is the data controller and the user authorities in terms of IT security, control and self-monitoring thereof, for example by concluding agreements between the data controller and authorities accessing SIS II;

34. ensure that the SIS II data controller adopts security plan without delay;

35. ensure that the SIS II data controller undertakes the activities related to the self-monitoring of the processing of personal data in N.SIS on a regular basis;

36. ensure that the SIS II data controller analyses the log files on a regular basis in order to ensure the data protection monitoring;

37. ensure that the logs regarding query on N.SIS data are stored for no longer then for 3 years period following their creation foreseen in Article 12(4) of the SIS II Regulation and the SIS II Council Decision.

Done at Brussels,

For the Council
The President