Council of the
European Union

Brussels, 10 December 2020
(OR. en)

13764/20

Interinstitutional File:
2019/0267(NLE)

PARLNAT 134

NOTE

From:	General Secretariat of the Council
To:	National Parliaments
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2019 evaluation of Slovenia on the application of the Schengen acquis in the field of data protection

In accordance with Article 15(3) of Council Regulation 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, the Council hereby transmits to national Parliaments the Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2019 evaluation of Slovenia on the application of the Schengen acquis in the field of data protection.[1].

[1] Available in all official languages of the European Union on the Council public register, doc. 13588/20

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2019 evaluation of Slovenia 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 Slovenia remedial actions to address the deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2019. 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)8050.

(2) As good practice are seen, amongst others, dedicated data protection training provided to Police staff; the fact that the DPA has carried out a considerable number of SIS II and VIS supervisory activities; the structure of the VIZIS provides for a high level of data protection and ensures that appropriate safeguards are in place and that information on SIS II and VIS provided to data subjects online is very detailed and readily accessible.

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

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the SIS II, priority should be given to recommendations 8, 13 and 14. With regards to recommendation 13, as of now, the Police is carrying out log audits for very few users dating back a long time. Auditing of logs of more users dating back a shorter time will decrease the burden of explanation for the single users and at the same time ensure a more consistent monitoring of user actions in the SIS II.

(4) In light of the importance of complying with the Schengen acquis on data protection in relation to the VIS, priority should be given to recommendations 5 and 6.

(5) Furthermore, in order to ensure legal certainty, it is essential to swiftly adopt national laws specifying the General Data Protection Regulation (EU) 2016/679 and transposing the Law Enforcement Directive (EU) 2016/680. Outmost priority should therefore be given to recommendation 1.

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

Legislation

1. as a matter of urgency, adapt its national legislation to the provisions of the General Data Protection Regulation (EU) 2016/679 and should completely transpose the Law Enforcement Directive (EU) 2016/680.

Data Protection Supervisory Authority

2. ensure that the mandatory audits by the DPA are completed in due time, once there is sufficient basis for decision-making.

3. ensure to carry out a general VIS audit of the data processing in the national system at least every four years.

Visa Information System

4. conduct and document a risk assessment for the server room and mitigate risks to physical security.

5. evaluate whether a recovery site for SI.VIS and VIZIS data sets should be established at a different location from the main server.

6. perform regular self-auditing of the whole SI.VIS to ensure the correct operation and use of the system.

7. ensure that the DPO of the MFA is actively involved in projects concerning processing of personal data.

Schengen Information System

8. ensure that the deletion procedure for supplementary information in the SIRENE-application is carried out more frequently in regular intervals.

9. ensure that deletion procedures for supplementary information in the SIRENE-application are documented in writing and accessible to the DPO and the DPA.

10. ensure that deletion procedures are carried out automatically in order to ensure that deletion takes place after the expiry of retention periods.

11. conduct and document a risk assessment for the Police data center and the Police server rooms and mitigate the highest risks to physical data security.

12. evaluate whether it is necessary to grant as many employees access to the server rooms in the Police data center and ensure that access rights are restricted to employees who need to physically access the server racks as part of their job function.

13. carry out more frequent log audits of access to and processing of SIS II-data.

14. ensure that retention periods of logs are respected and logs dating back more than three years are deleted, in line with the provisions of Article 12 (4) of the SIS II Decision and the SIS II Regulation.

15. carry out regular self-monitoring of the compliance with the SIS II data protection rules, in line with the provisions of Article 13 of the SIS II Decision and the SIS II Regulation.

Rights of data subjects and awareness raising

16. ensure that inspections initiated by the DPA upon request of the data subjects are completed in time so that the data subjects are able to effectively exercise their right to administrative remedy.

17. facilitate the exercise of the data subjects rights by interpreting general requests that do not specify for which system(s) people seek to obtain access to their personal data, as also including personal data processed in SIS II.

18. improve the standard reply to access to information requests, in cases where access is restricted.

19. ensure a proper legal basis in national law for restricting data subjects rights derived from the SIS II Decision.

Done at Brussels,

For the Council
The President