Council of the European Union

Brussels, 22 February 2022
(OR. en)

6426/22

Interinstitutional File:
2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	21 February 2022
To:	Delegations
No. prev. doc.:	5893/22
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2019 evaluation of **Poland** 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 2019 evaluation of Poland on the application of the Schengen acquis in the field of data protection, adopted by the Council at its meeting held on 21 February 2022.

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.

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2019 evaluation of Poland 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) In accordance with Regulation (EU) No 1053/2013, an evaluation to verify the application of the Schengen acquis in the field of the protection of personal data in Poland was 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(2021)9100.

(2) In view of the outcomes of the evaluation, it is appropriate to recommend to Poland certain remedial actions to address the deficiencies identified.

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

(3) As good practices are seen, in particular: the national legal framework, which allows the President of the Polish data protection authority (DPA) to appoint independently his or her deputies as well as the members of the Advisory Council; that the candidates for the position as President of the DPA have to undergo a public hearing in the Parliament, which is also broadcasted via the official channel of the Parliament on the internet; frequent control activities as regards external service providers, with involvement of the data protection officer, and frequent controls of consulates; the commitment to training and development of staff including on data protection, for end users of national Shengen Information System (N.SIS) and SIRENE Bureau staff; the security measures implemented on the premises of both data centres hosting N.SIS and national Visa Information System (N.VIS).

(4) In light of the importance of complying with the Schengen acquis on the protection of personal data in relation to the Visa Information System (VIS) and Schengen Information System (SIS), priority should be given to implementing recommendation 11, 12, 13, 20, 21 and 22 as set out in this Decision.

(5) Pursuant to Regulation (EU) No 1053/2013, this Decision should be transmitted to the European Parliament and to the parliaments of the Member States and Poland should, within three months of its adoption, 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 Poland should:

Legislation

1. clarify explicitly the applicability of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - 'GDPR') to the processing of personal data in N.VIS and N.SIS where relevant;

Data Protection Authority

2. ensure that Article 174 of Data Protection Act of 2018 and Article 106 of the Law Enforcement Data Protection Act of 2018 which stipulates the maximum limit of expenses per given year do not limit the budget of the Polish data protection authority (DPA) below the sums allocated in state budget for a given year;

3. ensure that the DPA better plans and organises its numerous inspections of the N.SIS II to ensure that all processing operations of the N.SIS II and all relevant entities are covered and that the inspections result in a comprehensive audit of the N.SIS II as provided for in Article 44(2) of the Regulation (EC) No 1987/2006;

4. ensure that the DPA conducts a comprehensive inspection of the N.VIS to fulfil fully its tasks in accordance with Article 41(2) of the Regulation (EC) No 767/2008;

Data Subjects' Rights

5. ensure that statistics of the DPA related to the exercise of the data subject rights are improved and differentiate complaints from requests, the system they refer to (SIS or VIS), the subject matter, as well as the type of request (correction, deletion, access);

6. ensure that the data controller adopts a more proactive approach with regard to providing information on the rights of the data subjects in relation to VIS data;

7. ensure that the SIS and VIS data controller (National Polish Police - Central Technical Authority for the National IT System (CTA NITS)) publishes standard forms for requests for exercisisng the data subjects rights;

Visa Information System

8. ensure that the records of access to the VIS contain also information about the justification of that access;

9. reassess the list of authorities with access to VIS and their access rights to VIS data, in view of their competences and use of such data in practice;

10. in light of the multitude of VIS data controllers set up by the national laws and contractual provisions, and given the multitude of actors involved, clarify the relationship between the authorities involved in the process of issuing visas and the authorities processing the VIS data, as well as responsibilities of those authorities for the data processing;

11. ensure that, to make full use of the log files kept, VIS log files are analysed regularly for data protection monitoring;

12. adopt a VIS security plan covering a physical security of the second data site as well as other IT security aspects of National IT System including the N.VIS system;

13. bring the retention period of logs on applications related to VIS (in particular in applications 'Pobyt' and 'ZSE 6') in line with the time limits of Article 34(2) of Regulation (EC) No 767/2008 and Article 16 of the Council Decision 2008/633/JHA;

Schengen Information System II

14. ensure that the N.SIS II controller sets up a central user management system that allows an effective self-monitoring without the need to consult logs at the institutions which are end-users of N.SIS II system;

15. ensure that, to make full use of the log files kept, SIS log files are analysed regularly for data protection monitoring;

16. ensure an automated notification of IT security events and self-monitoring activities of the data controller in order to further improve security;

17. ensure that technical measures also include blocking the usage of USB devices or sticks, by blocking all USB ports on SIS workstations;

18. consider to have the data protection officer (DPO) of the Ministry of Interior proactively and regularly involved in monitoring the processing of SIS and VIS data through monitoring audit logs;

19. ensure that the SIS data controller provides to the DPA the personnel profiles of all authorities with access to SIS;

20. bring the retention period of logs in the applications with access to SIS data in line with Article 12(4) of the Regulation (EC) No 1987/2006 and Article 12(4) the Council Decision 2007/533/JHA;

21. ensure that, in accordance with Article 10 of the Regulation (EC) No 1987/2006 and Article 10 of the the Council Decision 2007/533/JHA the SIS data controller adopts a SIS security plan;

22. ensure that the broad range of institutions with access to SIS II data is reviewed, so as to ensure that only institutions that need to have access, in view of their competences and practical needs, can access the data;

Public awareness

23. ensure that the websites of the DPA and the Police provide information about data subjects' rights in relation to VIS data.

Done at Brussels,

For the Council
The President