Council of the European Union

Brussels, 10 December 2020
(OR. en)

13743/20

Interinstitutional File: 2019/0277(NLE)

PARLNAT 131

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 2018 evaluation of Estonia 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 2018 evaluation of Estonia 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. 12870/20

COUNCIL IMPLEMENTING DECISION

setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of Estonia 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 Estonia remedial actions to address 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)9090.

(2) As a good practice, the on-site team welcomed the practice of Police and Border Guard Board (PBGB) and Estonian Data Protection Inspectorate (EDPI) of accepting digitally signed requests from the data subjects, that the PBGB provides the statistics concerning the requests of the data subjects to EDPI on a quarterly basis and a practice of Ministry of Foreign Affairs (MFA) to perform auditing of up to 5 consulates each year.

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

(3) In light of the importance to comply with the Schengen acquis, in particular the obligation to ensure and carry out effective supervision and to ensure necessary security measures, priority should be given to implement recommendation(s) 1, 2, 5, 16 and 17 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, Estonia shall, pursuant to Article 16, paragraph 1 of Regulation (EU) No 1053/2013, establish an action plan to remedy the deficiencies identified in the evaluation report and provide this to the Commission and the Council,

HEREBY RECOMMENDS:

that Estonia should

Legislation

1. properly implement the EU data protection reform as soon as possible;

Data Protection Supervisory Authority

2. ensure that the Estonian Data Protection Inspectorate (hereinafter "EDPI") finalises audits relating to the processing of the personal data within Schengen Information System II (hereinafter "SIS II") without delay;

3. ensure that future audits of processing of the personal data in SIS II and VIS are fully comprehensive and are conducted in line with international audit standards. In particular, the EDPI should, in the context of VIS audit, carry out inspections in consular posts and in External Service Providers' premises;

4. ensure that the follow up of inspections carried out by EDPI 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 EDPI about the implementation of the recommendations within a prescribed time frame;

5. ensure that the EDPI frequently conduct an analysis of logs of operations related to SIS II and VIS data, including access logs, for data protection monitoring;

Rights of Data Subjects

6. ensure that the Police and Border Guard Board's (hereinafter "PBGB") and EDPI's replies to data subjects' access requests contain information about the right to file a complaint to EDPI and to the court;

7. ensure that the positive answer provided to the data subjects in reply to their access request not only informs the data subjects that their data are processed in SIS II, but also informs them on the content of the data processed, by providing copy of the data;

8. provide clear information to data subjects about the identity of the data controller for processing of their personal data in the framework of issuing Schengen visas on the visa application forms;

9. provide to data subjects information about their rights in relation to VIS data not only in the harbours, but also at the Border Guard Station's premises;

Visa Information System

10. clarify the situation concerning the controllership of the processing of personal data in national VIS in particular, by clarifying the role of the Ministry of Interior (hereinafter "MoI"), Police and Border Guard Board, and Ministry of Foreign Affairs (hereafter "MFA") and by clarifying the allocation of responsibilities related to the processing of personal data amongst those authorities;

11. ensure that the contract between MFA and External Service Provider (hereinafter "ESP") clearly indicates that inspections to ESP premisses can be performed by the EDPI;

12. ensure that logs of the operations related to VIS data, including access logs and logs stored in all applications relevant for processing the VIS data (such as PIKO, KOMET, POLIS 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 the periods defined in Article 34(2) of VIS Regulation and Article 16 of the VIS Council Decision;

13. take the necessary steps to strengthen self-auditing of the compliance with the VIS acquis by MFA, in particular, in respect of effectiveness of the security measures and monitoring the lawfulness of the processing of personal data, amongst other by actively involving the Data Protection Officer of the MFA in tasks aiming to this end;

14. ensure that the VIS data controller(s) perform the self-monitoring of the processing of VIS personal data on a regular basis, including by analysing the log files on a regular basis in order to ensure the data protection monitoring; the data controller(s) should be encouraged to use dedicated tools for automatically searching the logs by different criteria to support monitoring and validating the accurateness of data processing;

15. 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 access to VIS data for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences respect the requirements and procedure established therein;

Schengen Information System

16. ensure that logs of the operations related to SIS data, including access logs and logs stored in all applications relevant for processing the SIS data (such as POLIS, UUSIS, PIKO, KOMET applications) are stored for no longer than for 3 years period following their creation as foreseen in Article 12 (4) of the SIS II Regulation and of the SIS II Council Decision, unless needed for ongoing monitoring procedures;

17. ensure the implementation of the recommendation from the previous Schengen Evaluation and provide for the automated deletion of SIS logs without delay;

18. ensure that PBGB enhances its activities related to the self-monitoring of the processing of personal data in N.SIS and performs such self-monitoring on a regular basis;

19. ensure that PBGB analyses the log files on a regular basis in order to ensure the data protection monitoring; the PBGB should be encouraged to extend the use of dedicated automated log analysis tools to that end;

20. examine the policy regarding the users' access to SIS data where all applications enable their users to have access to all SIS alerts, and when necessary revise user profiles and users access rights in line with Article 28 of SIS II Regulation and Article 43 of SIS II Council Decision and with Article 10 (1) (g) of SIS II Regulation and SIS II Council Decision, and define the scope of user access to SIS data according to what is strictly necessary for their tasks;

Public Awareness

21. ensure that the Guide for exercising the right of access adopted by the SIS II Supervision Coordination Group is available on the EDPI's website.

Done at Brussels,

For the Council
The President