Council of the
European Union

Brussels, 25 January 2021
(OR. en)

5533/21

Interinstitutional File:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	14247/20
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2019 evaluation of **Hungary** 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 Hungary on the application of the Schengen acquis in the field of data protection, adopted by written procedure on 21 January 2021.

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 Hungary 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 Hungary 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(2020)8170.

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

(2) As good practices are seen amongst others that the budget of the National Data Protection and Freedom of Information Authority (hereafter NAIH) has seen a constant increase, that the SIRENE Bureau complied with the recommendations of the previous Schengen data protection evaluation in 2012 and now refers to the possibility for data subjects to file a complaint to the NAIH; that the Ministry of Foreign Affairs and Trade (MFAT) refers also to judicial remedy; that the information provided on the NAIH website is comprehensive, useful and available, easily accessible and clear in terms of language; that the MFAT has taken efforts to manage and formalise the different aspects of information security; that the MFAT has a solid and comprehensive security plan and that the templates for exercising Schengen Information System (SIS) II data subjects' rights are available in several languages (Hungarian, English, German, French and Russian).

(3) No indication of priority for implementation of the recommendations should be given.

(4) This Decision should be transmitted to the European Parliament and to the parliaments of the Member States. Within six months of its adoption, Hungary should, pursuant to Article 16(8) of Regulation (EU) No 1053/2013, provide the Commission with an assessment of the (possible) improvements and with a description of required actions,

RECOMMENDS:

that Hungary should

Data Protection Authority (NAIH)

1. ensure that the NAIH when supervising compliance with SIS II legislation will also carry out regular inspections of SIS II alerts;

2. ensure that the NAIH will follow up on the Findings and Recommendations from the SIS II inspections and audits from previous supervisory measures and that those will also be considered in the 2019 inspection plans;

3. ensure that the NAIH conducts a comprehensive follow-up on the actual implementation of the recommendations from Visa Information System (VIS) supervisory activities;

4. ensure that the NAIH's VIS supervisory activity covers all the data protection aspects of the national visa system including the processing by External Service Providers;

Rights of data subjects

5. broaden the scope of Annex 9 of 15/2013 government decree (which establishes a specific template to exercise data subjects' access rights) to establish also templates for the exercise of the other data subjects' rights like correction and deletion;

6. ensure that the Hungarian authorities (National Directorate-General for Aliens Policing - OIF) clarify their procedures related to the assessment of requests of data subjects, in particular when limiting rights to rectification or to erasure and align them with the applicable Union and national law;

Visa Information System

7. ensure that privileged VIS users are sufficiently monitored; in this light organisational and technical measures may be required to monitor privileged users;

8. increase the frequency of the business continuity management (BCM)/disaster recovery plan (DRP) tests, in particular for MFAT;

9. ensure that, until the secondary IT-site is implemented, on the short term all of the backup of IT should not be stored at the same premise as the server room, but at an off-premise location;

10. increase the Rack access security;

11. regularly perform a security review of the internally developed encryption system (MFAT);

Schengen Information System

12. increase the physical security of the data centre building by covering also the 2nd exit/entry with camera surveillance and enhance the physical security of the racks in the server room;

13. regularly perform security reviews of the SIS II user access management system;

14. ensure the use of an uniform general set of directives/guidelines regarding information security for the N.SIS (e.g. password policy, …);

15. ensure that the SIRENE Bureau in cooperation with the National Archive explores the possibilities for a more frequent selection procedure concerning the data retention procedure;

16. increase the frequency of the business continuity management (BCM)/disaster recovery plan (DRP) tests;

17. ensure that the Hungarian National Police Headquarters (OFRK), and in particular N.SIS Office and SIRENE Bureau, install a solution for monitoring privileged users;

18. ensure that the SIRENE Bureau takes a more active role in coordinating the quality verification of the information entered in the SIS II as described in Article 1.15 of the SIRENE Manual;

Public Awareness

19. ensure that the MFAT clearly defines the data controller(s) for the purposes of VIS. To ensure transparency and to allow individuals to exercise their rights, it is important that data subjects are properly informed of the responsibilities of each individual data controller;

20. ensure that the ORFK provides regular updates to the English version containing the section on SIS;

Done at Brussels,

For the Council
The President