Council of the
European Union

Brussels, 22 October 2020
(OR. en)

12169/20

Interinstitutional File:
2020/0250(NLE)

SCH-EVAL 161
SIRIS 85
COMIX 492

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	20 October 2020
To:	Delegations
No. prev. doc.:	11281/20
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 the **Schengen Information System**

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 the Schengen Information System, adopted by written procedure on 20 October 2020.

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 the Schengen Information System

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 the Schengen Information System (SIS) 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) 1200.

(2) The on-site team considered the automatic notification about the creation, update or deletion of alerts by the SIRENE Bureau to the issuing or requesting authority; the pop-up windows highlighting the presence of aliases, misused identities and links in some of the main query applications; the roll-out of smartphones to query SIS; and the possibility of using smartphones and mobile devices with documents readers as backup solution in case of breakdowns, as best practices.

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

(3) In light of the importance of complying with the Schengen *acquis*, in particular the obligation to ensure the principle of equivalence of results, priority should be given to implementing recommendation 1, 6, 7, 8, 9, 11 and 20.

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

National Schengen Information System (N.SIS)

1. revise the procedure of retention of logs in line with Article 12(4) of Regulation (EC) 1987/2006[2] and Council Decision 2007/533/JHA[3];

2. ensure that *IdomSoft* premises comply with the security requirements established in the Article 10 of Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA, by improving facilities access control, data media and data access control, storage control and user control in relation to SIS data;

3. ensure that officers at the technical N.SIS locations have clear procedures and channels in place to communicate with eu-LISA staff;

[2] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).

[3] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

SIRENE Bureau

4. further automate the hit reporting procedure and communication between authorities using SIS and the SIRENE Bureau;

5. develop a tool for the collection of statistics as outlined in Annex V to the SIRENE Manual [4];

Applications querying SIS

6. align the values displayed in the "reason for request" of alerts for specific check converted into discreet checks in the application used by border police, with the "reason for request" for discreet checks set out in Annex III to the SIRENE Manual in line with Article 37(4) of Decision 2007/533/JHA;

7. ensure that the application used by border police displays the "action to be taken" and pictures in the alert in case of a hit in SIS;

8. ensure that the application used by border police can retrieve alerts with more than one given name in the relevant field during manual searches;

9. upgrade the police case-management system to enable queries on documents using just the first name and the last name of the person;

10. ensure that links on SIS alerts are sufficiently visible for the end-user in the main screen of the police case-management system;

11. ensure that the smartphone application can query all types of SIS alerts on objects;

12. upgrade the smartphone application to ensure that it can be used to query all kind of objects and that it highlights "terrorism related activity" in case of a hit on relevant SIS alerts;

[4] Commission Implementing Decision (EU) 2016/1209 of 12 July 2016 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (OJ L 203, 28.7.2016, p. 35–83).

13. ensure that the smartphones used to query SIS are equipped with anti-virus software and can only connect to secured wifi signals;

14. upgrade the the case-management application so that SIRENE officers may perform multi-category queries on objects;

15. consider making the photo affixed to the misused identity victim extension within the central register for wanted persons and objects immediately visible to the end-user;

16. ensure that when "immediate action" is part of the alert, this remark is properly highlighted on the screen of all query applications;

17. ensure that information about the presence of different identities is displayed in a coherent way in all the applications by aligning query functionalities in all the applications querying SIS;

18. consider connecting the Automatic number-plate recognition system (ANPR) to SIS;

Use of SIS

19. consider authorising the carrying out of specific checks on Hungary's territory;

20. ensure that the National Directorate General for Aliens Policing can attach the relevant fingerprints and other biometrics to its alerts whenever available at national level;

21. consider further integration of SIS usage into relevant processes and procedures of the National Tax and Customs Administration;

22. ensure that passengers outside of the border control booths at the first line in the motorway border crossing points cannot see the SIS data in the computers inside the booths;

23. ensure that common procedures are followed at the external borders for the transfer of information from the first line to the second line after a hit via the application used by border police;

Training

24. ensure that all end-users are aware about the availability of information on SIS and how to access this information;

25. ensure awareness training for all end-users on the use and specific displaying of links and on the procedures to request their creation;

26. intensify the training and promotion on the use of discreet checks for prevention, investigation and intelligence purposes for Criminal Investigation units;

27. consider organising training for the SIRENE Bureau, the Counter-Terrorism Centre (TEK) and the Constitution Protection Office (AH) aiming at improving the specific use of SIS by these authorities.

Done at Brussels,

For the Council
The President