Council of the European Union

Brussels, 9 April 2018
(OR. en)

7425/18

Interinstitutional File:
2018/0016 (NLE)

PARLNAT 73

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2017 evaluation of Sweden on the application of the Schengen acquis in the field of the Schengen Information System

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 2017 evaluation of Sweden on the application of the Schengen acquis in the field of the Schengen Information System[1].

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

ANNEX

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2017 evaluation of Sweden 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[2], and in particular Article 15 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The purpose of this this decision setting out a recommendation is to recommend to Sweden remedial actions to address deficiencies identified during the Schengen evaluation in the field of the Schengen Information System carried out in 2017. 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(2018)106.

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

(2) The quick response time of SIS during the visit with ranking the possible hits according to the percentage as they match to the queried data, the access management single sign-on method to the system, the easy and user-friendly display of SIS alerts on mobile devices and the fact that the internal hit reporting form is very user-friendly, are to be considered as best practice.

(3) In light of the importance to comply with the Schengen acquis, in particular the obligation to implement all SIS alert categories and functionalities, to integrate SIS queries into the police check application, to provide end-users adequate training as well as to develop the capability to monitor the availability of the system and the performance of the end-users, priority should be given to implementing recommendations 1-6, 9-13 and 21-27.

(4) This decision setting out a recommendation should be transmitted to the European Parliament and to the parliaments of the Member States. Within three months of its adoption, the evaluated Member State 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 Sweden should

1. resolve the data consistency discrepancies between its national copy and the Central SIS that can be experienced with regard to links as well as alerts to fulfil the requirement of full harmonisation and equivalence of results in accordance with Articles 9 and 15 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)[3] and 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)[4];

[3] OJ L 205, 7.8.2007, p. 69.
[4] OJ L 381, 28.12.2006, p. 9.

2. ensure that end-users are systematically consulting SIS when carrying out a police check by integrating the SIS and the national queries;

3. implement the linking functionality, in accordance with Article 52 of Council Decision 2007/533/JHA and Article 37 of Regulation (EC) No 1987/2006 to enable end-users to create links between alerts in case of an operational need;

4. ensure that the competent judicial authorities start to create alerts for judicial cooperation in criminal matters, in accordance with Article 34 of Council Decision 2007/533/JHA;

5. ensure that all available information is uploaded systematically to the relevant alerts on persons;

6. ensure that the mobile devices display whether an alert was issued under Articles 36(2) or 36 (3) of Council Decision 2007/533/JHA as well as links and the photo of the victim of the misused identity;

7. improve the display of information concerning the description and explanation on misused identity in the fixed terminals in order to clearly show that the alert relates to a misused identity and distinguish the victim from the perpetrator;

8. highlight the indication in the SIS-applications that the discreet or specific check alert was issued for immediate reporting;

9. ensure that all end-users during their basic training and afterwards during their career periodically receive adequate training on SIS, including its scope, use, functionalities, the different types of identities, the actions to take and the use of the SIS application;

10. ensure the updating of the online training material following the latest enhancements of SIS;

11. increase the awareness of the SIS among investigators in the regional units about the possibility to create alerts for discreet and specific check;

12. ensure that all end-users are aware of the hit procedure and the action to take in case of alerts issued for immediate reporting under Articles 36(2) or 36 (3) of Council Decision 2007/533/JHA;

13. involve the SIRENE staff in the end-user training and in the elaboration of the training content;

14. establish a monitoring mechanism within the SPOC ensuring that SIS alerts on persons are created when a corresponding national alert is created and a request for the creation of a SIS alert is sent by the competent authorities.

15. make the procedure for the creation of refusal of entry alerts more efficient by ensuring that national and SIS alerts are created at the same time within the same transaction;

16. adopt legislation allowing the creation of refusal of entry alerts on third-country nationals who are not present on the territory;

17. implement a technical solution for the automatic creation of alerts on firearms when a corresponding national alert is created;

18. implement the indication of urgency of incoming SIRENE forms in the case management system used by the SPOC;

19. enhance the knowledge of the SPOC operators on the different forms of identities in SIS;

20. revise and improve the translations of the SIS code tables in Swedish concerning the warning markers or the action to take by involving the SIRENE Bureau in the translation;

21. establish an accurate system of monitoring the use of SIS by creating statistical reporting on queries and hits in a break-down according to end-users;

22. provide accurate statistics on the use of the consultation procedure of Article 25 of the Schengen Convention;

23. establish a monitoring mechanism concerning the availability of N.SIS and the end-user applications and obtain reliable statistics in this regard;

24. enhance the availability of the border application and establish internal incident reporting allowing to measure the availability of the end-user applications;

25. in order to ensure higher availability of N.SIS and ensure business continuity, install a second connection to the sTesta network (TAP);

26. establish a solid and detailed business continuity plan and regularly test the business continuity solution and the related procedures;

27. update the security plan of 2011 in accordance with the requirements of the second generation of SIS;

28. define procedures and responsibilities for the customs authority concerning the use of SIS.

Done at Brussels,

For the Council
The President