Council of the European Union

Brussels, 4 October 2022
(OR. en)

12890/22

Interinstitutional File:
2022/0187(NLE)

PARLNAT 149

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 2021 evaluation of the **Netherlands** 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 2021 evaluation of the Netherlands 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. 12569/22

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2021 evaluation of the Netherlands 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(3) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) A Schengen evaluation in the field of personal data protection was carried out in respect of the Netherlands in April 2021. 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(2022)1700.

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

(2) As good practices are seen in particular: that the data protection authority's (DPA) secretariat staff members working with the issues related to Visa Information System (VIS) and Schengen Information System (SIS) receive appropriate training, which is customised for each person individually; the effectiveness of the security measures taken as regards to the premises of the SIS II equipment and the logistical/physical access thereto, ensuring a very high level of protection; the wide-ranging training concept of the National Police (NP) and in particular, the provision of e-learning modules and the comprehensive training strategy for new staff members, specifically at the SIRENE Bureau; the decentralised structure of personal data protection monitoring where contact persons for the issues regarding personal data protection are available in every unit of the police whilst two data protection officers (DPOs) are in charge of general supervision; the overall compliant technical security measures on VIS (network, firewalls, user management, access list on the IP addresses as an extra security measure) and in particular the precise and effective security measures provided by the NP; the active involvement of the DPO of the Ministry of Foreign Affairs (MFA) in issues related to personal data protection and security in the visa issuing process; the authorities' efforts for training and raising awareness of staff on personal data protection and security issues on VIS; that the MFA monitors External Service Providers (ESPs) on the basis of a check-list; the active involvement of the DPO of the MFA in issues related to personal data protection and data security in the visa issuing process; the fact that replies from the NP concerning SIS II are given also in English and answers provided to the data subjects inform them if their data is not contained in SIS II; that the data subjects requests on VIS addressed to the MFA do not have to be submitted only in Dutch and replies can be given in certain foreign languages.

(3) Recommendations should be made on remedial actions to be taken by the Netherlands in order to address deficiencies identified during the evaluation. In light of the importance of complying with the Schengen *acquis* on personal data protection and specifically on the supervision by the DPA and on the retention period of logs priority should be given to implementing recommendations 4, 5, 7, 10 and 15.

(4) This Decision should be transmitted to the European Parliament and to the national Parliaments of the Member States. Within three months of its adoption, the Netherlands should, pursuant to Article 16 (1) of Regulation (EU) No 1053/2013, establish an action plan listing all recommendations to remedy the deficiencies identified in the evaluation report and provide that action plan to the Commission and the Council.

RECOMMENDS:

that the Netherlands should:

Data Protection Authorities

1. ensure that the DPA has adequate resources to fulfil the tasks entrusted to it under the SIS II and VIS *acquis*;

2. establish legally binding and transparent provisions for appointing board members involving an objective selection committee and adopt the binding standard protocol containing rules about the selection of the members of the DPA (including that the open call of interest contains the requirements for the position);

3. ensure that inspections concerning the SIS supervision are carried out more frequently in order for the DPA to fulfil its tasks of comprehensively monitoring the lawfulness of processing of personal data in connection to SIS II;

4. ensure that N.SIS II audits are carried out either by the DPA or by an external auditor within a four-year cycle;

5. ensure that the DPA or the auditing company also make a thorough inspection of the server rooms and analysis of log files in order to fulfil the requirement of carrying out an audit of personal data processing operations in connection to N.VIS;

6. ensure that inspections concerning the VIS supervision are carried out more frequently in order for the DPA to fulfil its tasks of comprehensively monitoring the lawfulness of processing of VIS personal data;

7. ensure that the audits of the national visa system is carried out either by the DPA and/or by an external auditor within a four-year cycle;

Schengen Information System

8. establish a systematic review implemented by the NP of the single authorisations to access the N-SIS II;

9. consider initiating a regular control of the log files by a body which is more independent than the Security Operations Center, such as the privacy officers or the DPOs;

10. put in place relevant national provisions and retention practices in accordance with the Schengen *acquis* to comply with Art. 12(4) and (5) of Regulation 1987/2006 (SIS II Regulation)[1] and Article 12(4) of Council Decision 2007/533 (SIS II Council Decision)[2];

Visa Information System

11. consider establishing a common security plan for the visa issuing process applicable to all authorities involved;

12. establish a proactive log audit including automatic log control tools at all chain partners of the visa issuing procedure;

[1] 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 L381, 28.12.2006, p. 4-23

[2] 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 L205, 7.8.2007, p. 63-84

13. create a legal basis for the extensive information-supported decision-making and the Ministry of Foreign Affairs consult the DPA as soon as possible on the requirements under EU and national personal data protection law for the use of the BAO database;

14. ensure that any personal data still kept in the local warning lists are erased and, consequently, the still existing functionality in N.VIS on that subject matter is removed;

15. ensure the retention period for log records provided in Article 34 (2) of Regulation 767/2008 (VIS Regulation)[1] is respected;

Public Awareness and Rights of Data Subjects

16. ensure that the website in English of the DPA is updated to make easily available to data subjects the templates for exercising their rights stemming from the SIS II *acquis* and to provide information on remedies in a clear and plain manner;

17. ensure that the website of the NP is updated to provide templates or forms for exercising data subjects´ rights in relation to SIS II and that the English version of the website provides information on SIS and the related data subjects' rights;

18. ensure that the website of the NP informs about an e-mail address to which SIS requests can be sent and adapt the wording to make clear that that requests can be sent both via post and email;

19. ensure that the website of the NP is updated to include information about possible remedies concerning the processing of personal data in connection to the SIS;

20. ensure that the English version of the refusal letter concerning a SIS data subject request informs the applicant about any legal remedies which might be taken;

[1] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation); OJ L218, 13.8.2008, p. 60-81

21. ensure that the website of the DPA is updated to provide more specific and readily accessible information on the redress in respect of the processing of personal data in connection to the VIS, especially on the right to lodge a complaint and judicial remedies. The website should clearly define the scope of the applicable procedures and explain the differences between the mediation and the complaint;

22. ensure that the part of the MFA website with regard to the processing of personal data in connection to VIS is easy to find and provides model letters and information on all procedures available to data subjects;

23. ensure that the website "www.netherlandsworldwide.nl." provides more and specific information on the rights of data subjects regarding the processing of personal data in connection to VIS.

Done at Brussels,

For the Council
The President