Council of the European Union

Brussels, 19 March 2024
(OR. en)

7956/24

Interinstitutional File: 2024/0020(NLE)

SCH-EVAL 58
DATAPROTECT 151
COMIX 147

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7104/24
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2022 evaluation of **Luxembourg** 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 2022 evaluation of Luxembourg on the application of the Schengen acquis in the field of data protection, adopted by the Council at its meeting held on 19 March 2024.

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 2022 evaluation of Luxembourg 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 Luxembourg in March 2022. Following the evaluation, a report containing the findings and assessments, listing best practices and deficiencies identified during the evaluation was adopted by Commission Implementing Decision C(2024)300.

1 OJ L 295, 6.11.2013, p. 27.

(2) As good practices are seen in particular: the recent increase of the number of posts within the National Commission for Data Protection (Commission nationale pour la protection des données (CNPD) as well as the constant increase of the annual budget since 2016; that the budget of the CNPD is not part of any of the Ministries' budget; that the CNPD makes its own budget proposal to the Ministry of State, Department of Media, Connectivity and Digital Policy, which then transmits the proposal as such to the Ministry of Finance; that the police of Luxembourg has implemented a system where after every 1000 queries there is a pop-up window, where the end-user has to explain the query being made; that the police has implemented a clear methodology for self-monitoring, including monitoring both the end-users and external consultants; that the police has established a permanent position for the data protection officer; that Luxembourg authorities provide replies in different languages (German, French, Luxembourgish and English) on public awareness and data protection on SIS II.

(3) Recommendations should be made on remedial actions to be taken by Luxembourg 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 Data Protection Authority (DPA) and on the SIS II and VIS priority should be given to implementing recommendations 1, 4, 12, 13 set out in this Decision.

(4) In accordance with Article 15(3) of Regulation (EU) No 1053/2013, the Council should transmit this Decision to the European Parliament and to the national Parliaments of the Member States.

(5) Council Regulation (EU) 2022/922[2] applies as of 1 October 2022. In accordance with Article 31(3) of that Regulation, the follow-up and monitoring activities of evaluation reports and recommendations, starting with the submission of the action plans, should be carried out in accordance with Regulation (EU) 2022/922.

(6) Within two months of the adoption of this Decision, Luxembourg should, pursuant to Article 21(1) of Council Regulation (EU) 2022/922, establish an action plan to implement all recommendations and to remedy the deficiencies identified in the evaluation report. Luxembourg should provide that action plan to the Commission and the Council.

2 Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen *acquis*, and repealing Regulation (EU) N° 1053/2013, OJ L160 of 15.6.2022, p. 1.

RECOMMENDS

Luxembourg should:

Data protection authority

1. ensure that N.SIS II and N.VIS audits are carried out within the prescribed term of four-year cycle pursuant to the applicable EU legislation;

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

3. ensure that the VIS supervision inspections carried out by the data protection authority include personal data processing operations and data security at embassies, consulates and external service providers;

Schengen Information System

4. ensure that staff responsible for processing personal data are given mandatory and regular training in connection to SIS II as laid down in Article 14 of the SIS II Regulation, based on an established training plan;

5. create a written document about personal data protection and processing of personal data specifically dedicated to the SIS II, including all important information that the staff responsible should be aware of;

6. block the USB ports of the SIRENE workstations (at least for securised computers);

7. ensure that an efficient logging mechanism is in place where the SIRENE operators query the SIS on behalf of the end-users (in field officials);

8. delete more regularly temporary folders of the roaming windows profile of the SIRENE operator, which occur as a result of a query, and contain personal data, including biometric data;

9. implement mitigating measures (such as regular pop-up windows requiring the SIRENE operator to provide the reason for the search) also for alternative SIS search methods;

10. ensure that the physical security measures at the data center are complied with;

11. ensure that the logs which record the queries against the technical copy of SIS database (TC-NS-SIS) are stored for three years;

Visa Information System

12. establish a procedure to ensure that physical records at the Ministry of Foreign Affairs including Passport, Visa and Legalisation Office (BPVL-MAEE) premises are deleted timely, according to the VIS Regulation.

13. ensure that any individual user of the VIS receives prior training, based on a proper training plan;

14. revise the existing contractual agreements between the BPVL-MAEE and its external service providers, which currently require the ESPs to comply with the data protection standards of Directive (EU) 95/46/EC instead of Regulation (EU) 2016/679 (GDPR);

15. establish a comprehensive plan and methodology to ensure a regular and effective self-auditing and supervision of access obligations by all relevant authorities and extend the scope of the current self-auditing practice in relation to log checks;

16. establish a formal agreement or arrangement outlining the respective responsibilities of the MAEE and of the police, in relation to the processing of personal data in the VIS by the border police for the purpose of issuing short-stay visas;

Public awareness and rights of data subjects

17. ensure that the reply provided by the police in response to requests from data subjects concerning personal data processing in SIS II refers to the possibility to obtain redress before the national courts;

18. improve the accessibility of the information on SIS II on the website of the CNPD and make it user-friendly;

19. ensure that the website of the CNPD provides templates for access, deletion and rectification requests and the website of the police provides templates for deletion and rectification requests concerning personal data processing in the SIS II;

20. inform data subjects about the risks of sending personal data over the open Internet;

21. consider creating a secure channel for sending data subjects' requests for access, correction and deletion concerning SIS II personal data and provide information on that matter on the websites of the police and the CNPD;

22. provide clear information on the websites of the CNPD and the police about the exercise of data subject rights indirectly with the CNPD, when that right is limited in accordance with the national law;

23. correct the links of the website of the CNPD and the Grand Ducal Police addressing the European Commission;

24. consider providing some of the printed information, such as leaflets and signs, for the data subjects on the premises of police stations and make it visible and easily available;

25. correct the Schengen visa application form in use at the airport to identify the Ministry of Foreign Affairs (MFA) as data controller;

26. ensure that the website of the MFA provides for model letters to facilitate the exercise of data subjects' rights or contains a link to such model letters published on the website of the CNPD;

27. ensure that the website of the CNPD allows for easier and user-friendly access to information on how to exercise data subjects' rights vis-à-vis the MFA in the context of VIS;

28. ensure that information on SIS II and VIS, such as leaflets and documents addressing frequently asked questions is available in several languages (at least Luxembourgish, German, French and English) on the spot, including at the MFA, consulates and the police station at the airport, to inform data subjects and facilitate the exercise of their rights;

Done at Brussels,

For the Council

The President