Council of the European Union

Brussels, 24 September 2019
(OR. en)

12469/19

**Interinstitutional File: 2019/0169(NLE)**

**SCH-EVAL 158**
**DATAPROTECT 217**
**COMIX 428**

**OUTCOME OF PROCEEDINGS**

| | |
|---|---|
| From: | General Secretariat of the Council |
| On: | 20 September 2019 |
| To: | Delegations |
| No. prev. doc.: | 11906/1/19 REV 1 |
| Subject: | Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of **Latvia** on the application of the Schengen acquis in the field of **data protection** |

Delegations will find in the annex the Council Implementing Decision setting out a Recommendation on addressing the deficiencies identified in the 2018 evaluation of Latvia on the application of the Schengen *acquis* in the field of data protection, adopted by the Council at its meeting held on 20 September 2019.

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 2018 evaluation of Latvia 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 Latvia remedial actions to address the deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2018. 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(2019)5720.

(2) As good practice are seen amongst others the successful application to European Commission funding to improve public awareness and the fact that replies from the SIRENE Bureau are available in different languages and that answers are generally given in a short time.

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

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the Schengen Information System II (SIS II), priority should be given to recommendations 15 to 18.

(4) In light of the importance of complying with the Schengen acquis on data protection in relation to the Visa Information System (VIS), priority should be given to recommendations 9 and 11.

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

**Data protection supervisory authority**

1. ensure the complete independence of the Data Protection Authority (DPA) by adopting national legislation that complies with Chapter VI of the General Data Protection Regulation (hereafter 'GDPR'), in particular the procedure on the dismissal of the Director;

2. ensure that the Data Protection Authority receives sufficient funding and ensure an adequate level of employees in order for it to be able to fulfil all tasks entrusted to it under the Schengen Information System II (hereafter "SIS II") and Visa Information System (hereafter "VIS") acquis;

3. ensure that the audit of data processing operations in N.SIS as required by Article 44(2) of the SIS II Regulation and Article 60(2) of the SIS II Council Decision is carried out in a timely manner;

4. ensure that the audit of data processing operations in the NVIS is carried out as required by Article 41(2) of the VIS Regulation and Article 8(6) of the VIS Council Decisision;

5. ensure that future audits of SIS II and VIS are fully comprehensive and are conducted in line with international audit standards as required by SIS II and VIS acquis, and ensure that the necessary IT expertise is deployed for these audits;

6. ensure that the supervisory activities of the DPA in relation to the SIS II include regular controls of SIS II alerts;

7. ensure that the supervisory activities of the DPA in relation to the VIS include regular inspections of Consular Posts;

8. ensure that the DPA's multi-annual inspection plan includes other inspection activities than the mandatory audits of SIS II and VIS;

**Visa Information System**

9. ensure that log files are analysed regularly for the monitoring of the lawfulness of the data processing activities in line with Article 34(1) and (2) of the VIS Regulation;

10. clarify the role (data processor or joint controller) of the Ministry of Foreign Affairs (hereafter 'MoFA') - in relation to the Office of Citizenship and Migration Affairs (hereafter 'OCMA');

11. ensure more frequent self-auditing of processing activities within VIS by OCMA;

12. revise the contracts with external service providers in order to respect and align with the requirements laid down in the GDPR;

13. define clearly the tasks and powers of the OCMA and MoFA data protection officers, respectively;

14. Ensuring that online forms used in the context of a visa application include a data protection notice informing data subjects about the data processing activities and the applicable individual rights,

**Schengen Information System**

15. ensure that the police carry out self-auditing on a regular basis, in particular self-monitoring of logs;

16. generate national SIS II logs at a central level and ensure that the justification for the query can be established from the log;

17. Ensuring that log files are reviewed on a regular basis to check the lawfulness of data processing in line with article 12(2) SIS II Regulation and SIS II Council Decision.

18. minimize the security risk posed by the mobile application that allows access to SIS II through, for example, making access available only through a VPN service;

19. put in place a two-factor authentication system;

20. ensuring that production data is not used for test purposes and that only duly authorised users can carry out searches into the NSIS.

21. clearly define the tasks and powers of the data protection officer within the police, including his participation on internal monitoring activities, such as the monitoring of the effectiveness of the security measures;

**Rights of data subjects and awareness raising**

22. provide the DPA with the statistics concerning the exercise of data subject rights related to SIS II and VIS on a regular basis;

23. render more available information material such as the brochure 'Personal Data in the Schengen Information System' at the airport and other public places;

Done at Brussels,

*For the Council*
*The President*