Council of the European Union

Brussels, 24 September 2019
(OR. en)

12468/19

Interinstitutional File: 2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	20 September 2019
To:	Delegations
No. prev. doc.:	11904/19
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of **Lithuania** 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 Lithuania 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 Lithuania 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 Lithuania 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) 5700.

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

(2) As good practice are seen amongst others the fact, that the Data Protection Authority (DPA) provides advice and guidance to individuals who approach them instead of simply forwarding requests; provision of template letters for exercising Schengen Information System II (SIS II) and Visa Information System (VIS) related data subjects' rights; security measures implemented on the premises of the Information technology and Communications department under the Ministry of Interior (MoI) (ITCD -hosting N.VIS and N.SIS) are in general of high standard, providing a secure environment for storing data and for preventing possible incidents; training for VIS end users, in particular for consular staff before posting to embassies/consulates is well-developed; there is commitment to training and development of staff in particular a well-developed training including on data protection for end users of N.SIS and the SIRENE Bureau staff; the information provided by the DPA on its website in regard to the SIS II and VIS is very comprehensive, useful and in easily accessible language (available in several languages); the DPA's brochures on "*Personal Data Protection in the Schengen Information System*" and "*Personal Data Protection in the Visa Information System*" provide very good and accessible information on the processing of data in both databases and the related data subjects' rights as well as the strong involvement of the DPA in many conferences, trainings and other awareness raising events including to staff dealing with SIS II and VIS data processing.

(3) In light of the importance of complying with the Schengen acquis on data protection, in particular to ensure the complete independence of the DPA, priority should be given to implementing recommendation 1.

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

Data protection supervisory authority

1. in order to better ensure the complete independence of the State Data Protection Inspectorate (hereafter DPA) abolish the requirements to have the DPA's strategic action plan approved by the Minister of Justice and to consult the Minister of Justice on the annual action plan before the Director of the DPA may approve it; this is important also for ensuring that the budgetary procedure has no element of risk of violation of the independence of the DPA;

2. in order to better ensure the complete independence of the DPA, organise the bilateral meetings held on a regular basis between the Minister of Justice and the Director of the DPA in such a way that it could not result in a risk of direct or indirect influence of the Government on the DPA, which could endanger the independence of the DPA;

3. abolish all those elements of the accountability of the Director of the DPA to the Government and to the Minister of Justice which could result in a risk of direct or indirect influence by the Government and the Minister of Justice and could endanger the DPA's independence;

4. ensure that the DPA monitors the lawfulness of the processing of SIS II personal data more frequently;

5. ensure that, at least every four years, audits of data processing operations in N.SIS will be carried out by the DPA;

6. ensure that the DPA monitors the lawfulness of the processing of VIS personal data. The DPA should also inspect data processing operations and data security at the External Service Providers (ESPs) when it is inspecting embassies; this possibility should be specified in the contract between the Ministry of Foreign Affairs (MFA) and the ESPs;

7. ensure that, at least every four years, audits of data processing operations in N.VIS will be carried out by the DPA;

Rights of Data Subjects

8. ensure, that the 60-day deadline for replying to SIS II data subjects requests provided for in Article 41(6) of the SIS II Regulation and Article 58 (6) of the SIS II Decision will be respected until the new SIS acquis[2] will become fully applicable (latest by 28 December 2021)in which there are cross-references to the deadline for replying to data subjects requests foreseen in the General Data Protection Regulation (GDPR)[3] (30 days with possibility to extend by two further months when necessary);

9. clarify internal procedures on the responsibility of the involved authorities for dealing with SIS II data subjects' rights; this way staff could also be aware who to refer requests to;

---

2 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) N) 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312of 7.12.2018, p. 56 (see in particular Articles 66 – 71); Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312 of 7.12.2018, p. 14 (see in particular Articles 51 – 57).

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119 of 4.5.2016, p. 1.

10. ensure that MoI will be consistent in any final responses to individuals wishing to exercise their SIS II data subjects' rights, so that information is provided on their right to appeal to the DPA as well as the rights to seek judicial remedy throughout the courts;

11. clarify internal procedures on the responsibility of the involved authorities for dealing with VIS data subjects' rights; this way staff could also be aware who to refer requests to;

12. ensure that the MoI will be consistent in any final responses to individuals wishing to exercise their VIS data subjects' rights, so that information is provided on their right to appeal to the DPA as well as the rights to seek judicial remedy throughout the courts;

Visa Information System

13. take the necessary steps to ensure that the contracts between the MFA and the ESPs regulate in what way the Lithuanian DPA can be involved in the inspections conducted by the embassies/consulates and the MFA;

14. improve the self-monitoring by proactively checking logs on a regular basis in order to monitor the lawfulness of the processing of VIS personal data. The MoI should further develop the SIEM system for the automatic log control;

15. ensure that the DPO of the MFA will be more strongly involved in the development and provision of data protection training to MFA staff including those posted to embassies/consulates;

Schengen Information System II

16. remove the possibility of an end-user to log via the POLIS Browser into N.SIS with several devices at the same time;

17. ensure that smart cards for access to workstations of N.SIS users in the police will be introduced in order to enhance the level and standard of security;

18. ensure that the technical measures in place to prevent the use of USB sticks in SIRENE Bureau workstations will be fully applied and controlled periodically;

19. improve the self-monitoring by proactively checking logs from SIS II end-users of all concerned authorities on a regular basis in order to monitor the lawfulness of the processing of SIS II personal data; the MoI should further develop the SIEM system for the automatic log control;

20. ensure that data protection awareness of staff in relation to the handling of SIS II and VIS data is enhanced through regular refresher training sessions;

21. ensure that training and awareness raising of staff having access to N.SIS will be an area that the group of DPOs in the MoI will lead on. By this it could ensure that there is a continued structure and planning for the development of staff.

Public awareness

22. ensure that the links on the DPA's website concerning SIS II and VIS are updated on a regular basis;

23. ensure that the websites of organisation which have contacts with nationals of other countries such as the MoI, Police, State Border Guard Service, MFA and consular offices provide accessible and clear information on SIS II and VIS and the related data subjects' rights also in English;

24. ensure that when websites provide information on SIS II and VIS and the related data subjects' rights in English, that this information will be easier to find;

25. ensure consistency of the information on the exercising of data subjects' rights in relation to N.SIS II and VIS provided on the websites of the institutions which work with these systems;

26. add information on data processing and VIS related data subjects' rights to the EPM portal through which individuals provide details for visa applications.

Done at Brussels,

For the Council
The President