Council of the European Union

Brussels, 11 February 2021
(OR. en)

5904/21

**Interinstitutional File:**
**2020/0304(NLE)**

PARLNAT 21

**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 2019 evaluation of Slovakia 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 2019 evaluation of Slovakia 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. 5534/21

Council Implementing Decision setting out a

**RECOMMENDATION**

**on addressing the deficiencies identified in the 2019 evaluation of Slovakia 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 the Slovak Republic remedial actions to address the deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2019. 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(2020)8160.

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

(2) As good practices are seen amongst others that since the last Schengen Evaluation in 2012 the Data Protection Authority (DPA) has carried out SIS II supervisory activities on a regular basis according to a yearly planning and that a concept for the SIS II inspections for the next four years has been elaborated; that the DPA has carried out a considerable number of VIS inspections of consulates; the efforts of the DPA and the Ministry of Interior (MoI) to provide information to data subjects in electronic and printed materials; the multi-language versions of the information on Schengen related topics on the DPA's website and in the leaflets; that the DPA provides for templates for SIS and VIS data subjects' requests; that the SIRENE Bureau provides for responses to requests not solely in Slovak language, but also in English; that the Slovak authorities inform the data subjects if no data on them is stored in the SIS II; the very active VIS and SIS II log control by the inspection section of the Bureau of inspection service of the MoI; the very active role of the two staff members in the Ministry of Foreign and European Affairs's (MFEA) Security Department dealing with data protection issues; that the MFEA is providing data protection training to its staff, in particular before temporary posting for consular tasks and that the Security Department (in its role as DPO office) is providing this training; that the procedural and physical security set up for protecting SIS II data is on a high level; the very active role of the DPO and deputy DPO in the Data Protection Department of the Inspection Unit of the Bureau of Inspection Service of the MoI including on guidance and log control concerning SIS II; that the MoI is providing data protection training to all N.SIS II end users.

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the VIS, priority should be given to implementing recommendations 7 and 24.

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

**Data Protection Authority**

1. ensure that in order to reinforce the performance and effectiveness of the DPA, the DPA‘s budget and staff should be further increased;

2. ensure that the part of the overall state budget foreseen for the DPA should be clearly visible in order to guarantee that the DPA has a separate, public annual budget;

3. ensure that in the budgetary procedure the National Council should be made aware of the DPA’s position on its budgetary needs and the discussions held between the DPA and the Ministry of Finance (MoF) on the budget;

4. take measures so that the MoF cannot make any correlation between the budget and the amount of fines to be collected by the DPA as this might have an impact on the nature and prioritisation of the DPA’s work and thus affect its independence. It should be guaranteed that the budget of the DPA cannot be decreased during the calendar year in a situation where the estimated fines has not been fully collected by the DPA;

5. ensure that all tasks and powers provided for data protection authorities in Articles 57 and 58 GDPR will be granted to the DPA;

6. ensure that in addition to the regular supervisory activities carried out at the N.SIS office and the SIRENE Bureau the DPA supervises more end user authorities having access to SIS II;

7. ensure that the supervisory activities of the DPA in relation to VIS include the inspection of the Central Visa Authority (CVA) with regard to the data processing operations in the N.VIS. As the deadline for the first audit of the national visa system was October 2015, the DPA should carry out this still missing part of the audit as soon as possible;

8. ensure that the DPA inspects also the External Service Providers (ESPs) on a regular basis;

**Rights of data subjects**

9. should find an appropriate way for the DPA, the MoI and the MFEA to inform data subjects about the potential risks of submitting copies of ID cards and sensitive information via open internet. The MoI and MFEA are invited to consider offering to data subjects a secured electronic transmission channel for submitting such documents;

10. ensure that the 60-day deadline for replying to SIS II data subjects' requests laid down in Article 41 (6) of the SIS II Regulation and Article 58(6) of the SIS II Decision is respected until the new SIS acquis[1] 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 GDPR (30 days with possibility to extend by two further months where necessary);

11. consider to provide some of the printed information (leaflets/signs etc.) for the data subjects on the premises of police stations as well as to make it visible and easily available;

12. consider to provide e.g. an informal English version of the decisions of the DPA on complaints on SIS II data subjects' requests; this would help data subjects to better understand the decision and would thus strengthen the data subjects' rights;

13. ensure that the information on VIS data subjects' rights on the website of the MFEA is easier to find; the website should also provide for templates for the exercise of VIS data subjects' rights;

---

[1] 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)

14. ensure that the visa application form contains clear information about the different authorities that process personal data as part of the national visa system. In particular there should be information that the MFEA is the data controller;

15. provide physical information (leaflets/signs etc.) for the VIS data subjects on the premises of airports and other border control spots and make them visible and easily available;

16. ensure that the replies to data subjects concerning VIS personal data should provide information on the possibility to appeal against the reply before the DPA and the competent court;

17. take the necessary measures to clarify the MFEA's and the CVA's (MoI) responsibilities for dealing with VIS data subjects' requests and to make internal or methodological guidance for both entities; this information should be available for data subjects;

**Visa Information System**

18. take the necessary measures to increase the security level for accessing to the governmental environment and in particular the national visa applications at the MFEA and MoI (CVA) in particular by access to the national visa databases via multi-factor technology;

19. take the necessary measures to improve the physical and organisational security in the MFEA's N.VIS data centre in particular on the following aspects:

    – Provision of a visitor logbook at the entrance of the data centre for ICT staff, visitors or suppliers whose access should be limited;

    – Installing a system of fire extinction with gas (aragonite);

    – Installing water leakage detection,

    – Ensurance of dust free and orderly floor;

    – Locking of EU servers protection fence;

20. accelerate the procedure for setting up a new N.VIS data centre in another location and the resettlement of the data centre;

21. consider to change the local retention period of the N.VIS log files in the diplomatic and consular missions by setting a time period instead of the amount of MB;

22. consider to use automatic log control systems at the MFEA;

23. take the necessary measures so that diplomatic missions or the MFEA inspect the ESPs on a regular basis;

24. take the necessary measures to provide data protection training to local consular staff more systematically and in an uniform way;

25. ensure that the electronical visa application requests the same information as the paper visa application form (as laid down in Annex I of the EU Visa Code[1]);

**Schengen Information System II**

26. take the necessary measures to improve the security level for accessing to the N.SIS II in particular by using multi-factor authentication and only https-connections for access to the N.SIS II;

27. ensure that the MoI informs the DPA about any data breach which is likely to result in a risk to the rights and freedoms of natural persons. Furthermore the MoI should establish a register of personal data breaches;

[1] Regulation (EC) N) 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code); OJ of 15.9.2009, L243/1.

**Public awareness**

28. consider to put the DPA leaflets at the disposal of data subjects also at more accessible locations such as police stations, border control areas and consular premises;

29. consider to make DPA presentations, seminars and open door events also accessible for the large public in particular data subjects, as they are concerned by the information on SIS II and VIS;

Done at Brussels,

*For the Council*
*The President*