Council of the European Union

Brussels, 3 April 2019
(OR. en)

8138/19

**Interinstitutional File: 2019/0024(NLE)**

PARLNAT 31

**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 2018 evaluation of Switzerland 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 2018 evaluation of Switzerland 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. 7281/19

**ANNEX**

Council Implementing Decision setting out a

**RECOMMENDATION**

**on addressing the deficiencies identified in the 2018 evaluation of Switzerland 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[2], 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 Switzerland 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)200.

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

(2) As good practice are seen amongst others the guide on "Monitoring the use of the Schengen Information System (SIS)" developed by the Schengen Coordination Group established by the Swiss data protection authorities; that the website of the Office of the Federal Data Protection and Information Commissioner (hereafter FDPIC) contains very comprehensive specific model letters for exercising data subjects' rights related to Schengen Information System (hereafter SIS II) Visa Information System (hereafter VIS), as well as very good information in its frequently asked questions related to SIS II "Schengen … and your personal data" and to VIS "The Schengen VISA and your personal data"; the promptness of responses by the Federal Office of Police (fedpol) to data subjects' requests, particularly in light of the significant numbers of requests received; that security measures implemented on the premise of the IT Service Centre ISC-FDJP server room (hosting N-VIS and SIS II) are of high standard, provide a secure environment for storing data and for preventing possible incidents; the extensive efforts of fedpol with regard to the training and awareness raising for their staff including on data protection issues; the active involvement of the DPOs of fedpol in particular by providing training and advice on all questions concerning data protection and dealing with all data subjects' requests.

(3) In light of the importance of complying with the Schengen acquis on data protection in relation to the SIS II and the VIS, priority should be given to implementing recommendations 12 and 15 below.

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

**Data Protection Supervisory Authorities**

1. in order to better ensure the complete independence of the FDPIC consider to abolish – in the framework of the revision of the Federal Act on Data Protection - the possibility for the Commissioner of the Federal Data Protection and Information Commissioner (FDPIC) to have a secondary occupation;

2. in order to better ensure the complete independence of the DPA of the Canton Lucerne abolish the possibility to dismiss the Data Protection Commissioner of Lucerne on "justified grounds" (which can be grounds other than serious misconduct);.

3. strengthen the enforcement powers of the FDPIC, so as to enable it to directly take legally binding decisions;

4. strengthen the enforcement powers of the cantonal data protection authorities by giving them the right to directly take legally binding decisions;

5. allocate sufficient financial and human resources to the FDPIC in order for it to be able to fulfil all tasks entrusted to it under the SIS II and VIS acquis;

6. allocate sufficient financial and human resources to the DPA of the Canton Lucerne in order for it to be able to fulfil all tasks entrusted to it under SIS II and VIS acquis;

7. in order to better ensure the complete independence of the DPA of the Canton Lucerne enable the DPA of the Canton Lucerne to appoint its own staff according to its requirements;

8. in order to better ensure the complete independence of the FDPIC reform the budgetary procedure in such a way that the FDPIC has a real influence on the proposal for its budget before the general budget proposal is sent to the Parliament for discussion and adoption as well that the budgetary proposal of the FDPIC will be made known to the Parliament;

9. in order to better ensure the complete independence of the DPA of the Canton Lucerne reform the budgetary procedure in such a way that the DPA of the Canton Lucerne has a real influence on the proposal for its budget before the general budget proposal is sent to the Parliament for discussion and adoption; the DPA of the Canton Lucerne should be given budgetary autonomy and thus the right to influence and control budgetary decisions relating to it;

10. ensure that the FDPIC monitors the lawfulness of the processing of SIS II personal data more frequently. These inspections should continue to include the checking of log files but should cover also other data protection aspects of the structure and functioning of N-SIS II;

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

12. ensure that, at least every four years, audits of data processing operations in N.SIS will be carried out by the FDPIC; this audit should cover also the data processing operations in N-SIS II at the data controller of N-SIS II, thus fedpol including the SIRENE B and the N-SIS server; as the deadline for the first audit was April 2017 actions should be taken to fulfil this obligation as soon as possible;

13. ensure that the FDPIC monitors the lawfulness of the processing of VIS personal data more frequently;

14. ensure that the DPA of the Canton Lucerne monitors the lawfulness of the processing of Visa Information System (hereafter VIS) personal data more frequently;

15. ensure that, at least every four years, audits of data processing operations in the national system of VIS (ORBIS) will be carried out by the FDPIC. As the deadline for the first audit (October 2015) has not been met, action should be undertaken to fulfil this obligation by finalising the on-going audit as soon as possible;

**Rights of Data Subjects**

16. give careful consideration to how the SIS II related rights of data subjects living overseas can be more effectively provided as Swiss law requires that formal decrees (cases of refusal of access to personal data) must be sent to a Swiss address;

17. provide information on the websites of the fedpol and FDPIC about the possibility for data subjects of seeking a judicial remedy in cases where the deadline to provide a response to SIS II related data subjects requests (60 days) is not met;

18. ensure that all websites of the cantonal police authorities provide basic data protection information and a direct link to the Cantonal DPA's websites;

19. ensure that the various data protection supervisory authorities, at Federal and Cantonal level, are resourced adequately in order to fully undertake their obligation to upholding and supporting the exercise of data subject rights, including accepting complaints brought to them by individuals;

20. provide information on the legal basis for making a charge for the exercise of data subjects' rights (including information what might constitute a repetitive/abusive request) in the Schengen FAQs and on the websites of the fedpol, FDPIC and DPA of the Canton Lucerne and overseas missions/consulates;

**Visa Information System**

21. add data protection elements to the two months intensive training provided by the State Secretariat of Migration (SEM) for visa staff;

22. ensure that the SEM proactively checks logs on a regular basis in order to monitor the lawfulness of the processing of VIS personal data;

23. ensure that the SEM in general improves its self-auditing measures as required under Article 32 (2) k of the VIS Regulation and Article 9(2) k of the VIS Council Decision;

**Schengen Information System**

24. ensure that technical measures are put in place by fedpol in order to prevent the use of the USB ports of workstations with access to N-SIS II;

25. ensure that foreign missions, airports, police stations and cantonal migrations offices make paper versions of the leaflet "Schengen and your personal data" available to the general public on their premises;

26. check and redefine whether authorised N-SIS II users are technically able to be logged in at the same time via different means (e.g via a fixed workstation and a mobile device); update internal information security documents in order to avoid a simultaneous logging into N-SIS II via different means;

27. ensure that fedpol proactively checks logs on a regular basis in order to monitor the lawfulness of the processing of SIS II personal data

28. ensure that fedpol in general improves its self-auditing measures as required under Article 10 (1) k of the SIS II Regulation and Article 10 (1) k of the SIS II Council Decision;

**Public Awareness**

29. ensure that the information material on VIS data subjects' rights is easier to find and more clearly signposted beyond the FDPIC's website also by providing the websites of the SEM and the Cantonal police and Cantonal DPA equally in English;

30. ensure that foreign missions, airports, police stations and cantonal migrations offices make paper versions of the leaflet "Schengen and your personal data" available to the general public on their premises;

Done at Brussels,

*For the Council*
*The President*