Council of the European Union

Brussels, 19 December 2019
(OR. en)

15009/19

Interinstitutional File:
2019/0255(NLE)

SCH-EVAL 219
DATAPROTECT 303
COMIX 581

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	19 December 2019
To:	Delegations
No. prev. doc.:	14661/19
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2019 evaluation of the **Czech Republic** 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 2019 evaluation of the Czech Republic on the application of the Schengen acquis in the field of data protection, adopted by the Council at its meeting held on 19 December 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 2019 evaluation of the Czech Republicon 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 Czech 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(2019) 9040.

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

(2) As good practice are seen amongst others the fact, that templates are available in Czech and English on the website of the Data Protection Authority (hereafter DPA) to exercise the right of access or rectification with respect to the Visa Information System (hereafter VIS) and Schengen Information System II (hereafter SIS II); the DPA accepts data subjects' complaints in Czech and English and provides replies in English with respect to VIS and SIS II; the Ministry of Foreign Affairs (hereafter MFA) instructs consular posts (hereafter CPs) not to keep so-called "blacklists"; there is well developed data protection training for expatriate staff at CPs, which is organised in cooperation with the MFA's Data Protection Officer (hereafter DPO) and the DPA; the MFA has clear instructions for CPs on how to cooperate with External Service Providers (hereafter ESPs) in its "Technical and organisational handbook for cooperation with ESPs in processing Schengen visa applications"; the technical and organisational security measures with respect to the N.VIS are of high standard, including access management and log keeping; the IT organisation of the Police has a profound maturity level with reference to the different aspects of IT security, expressed in technical as well as organisational measures; the Police carries out log analysis where suspicious queries on N.SIS II are automatically detected and reported; the Police DPO Department regularly provides data protection training; the information provided by the DPA on its website with regard to SIS II and VIS is comprehensive and easily accessible; the DPA is strongly involved in conferences, trainings and other awareness raising events; the MFA's website provides information to data subjects in various languages.

(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 recommendation 3.

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

Legislation

1. implement the General Data Protection Regulation (GDPR)[1] and transpose the Directive 2016/680[2] as soon as possible into its national legal framework;

Data protection authority

2. ensure that the DPA in relation to SIS II carries out more frequent inspections of authorities entitled to access the SIS II (e.g.. the Aliens Department);

3. ensure that the supervisory activities of the DPA in relation to VIS include inspections of the Police, which operates and maintains the NS.VIS;

Rights of data subjects

4. ensure that the Police website contains templates for data subjects to exercise rights of access, correction or deletion;

5. 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;

---

1 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 119/1 of 4.5.2016

2 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89 of 4.5.2016

6. take measures that would facilitate non-Czech speaking data subjects to better understand replies provided to them by the Police in response to requests for access, correction or deletion concerning personal data processing in SIS II, for instance by providing an informal English or Russian version of such replies(depending on the request). This would strengthen the data subjects' rights;

7. consider a more accurate wording for replies by the Police to requests of access to personal data in SIS II where that data cannot be disclosed without prejudice to an investigation;

8. ensure that the visa application form contains clear information about the different data controllers that process personal data as part of the national visa system (the MFA with respect to EVC2 and the Police with respect to NS.VIS);

9. take measures that would facilitate non-Czech speaking data subjects to understand replies provided to them by the Police in response to requests for access, correction or deletion concerning personal data processing in VIS, for instance by providing an informal English or Russian version of such replies (depending on the request);

10. ensure that the English version of the DPA's website provides a template for lodging a complaint concerning personal data processing in the national visa system;

11. ensure that the website of the Police and the MFA provide templates for exercising data subject rights concerning VIS personal data processing;

12. ensure that the reply provided by the Police in response to requests from data subjects concerning personal data processing in NS.VIS contains a reference to the possibility to obtain redress before the national courts;

13. ensure that the reply provided by the MFA in response to requests from data subjects concerning personal data processing in EVC2 provides information about the possibility to obtain judicial redress before the national courts;

Visa Information System

14. lay down and document the different roles of the Police and the MFA in relation to personal data processing in the national visa system, in particular in light of the concepts of controller and processor and the allocation of responsibilities under the GDPR;

15. take the necessary measures for the MFA to ensure that the documentation concerning the EVC2 system security is kept up to date, that review cycles (e.g. annual risk assessment reviews) are observed and that the rules for registration and archiving of security documentation are fully respected;

16. take the necessary measures for the MFA to ensure that the data retention rules (reflecting the requirements of Annex X to the Visa Code) as laid down in the Concession Contract between the MFA and the ESPs are applied in practice;

17. provide systematic and uniform data protection training to local consular staff;

Schengen Information System

18. ensure that the documentation of security policies of the Police with respect to SIS II contains the version and approval status thereof;

19. consider the possibility for the Police of adding additional controls for the protection of biometrical information (such as more specific encryption techniques), taking into account the impact on performance of information systems;

Public awareness

20. ensure that the application form for Schengen visa, available on the website of the MFA, clarifies the responsibilities of the MFA, the Police and the Ministry of Interior with respect to personal data processing in the national visa system (in particular EVC2 and NS.VIS).

Done at Brussels,

For the Council
The President