Council of the European Union

Brussels, 24 June 2022
(OR. en)

10405/22

Interinstitutional File:
2021/0224(NLE)

PARLNAT 101

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 2020 evaluation of **Austria** 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 2020 evaluation of Austria 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. 10396/22

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2020 evaluation of Austria 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) A Schengen evaluation in the field of data protection was carried out in respect of Austria in November 2020. 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(2021)9200.

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

(2) As good practices are seen in particular: that since the last evaluation the staff of the Austrian data protection authority (DPA) has and still will be reinforced as well as that the budget has been increased; the controller-processor agreements in relation to VIS-data provide for a high level of data protection and ensure that the all parties implied in the VIS data processing have relevant data protection safeguards in place; the training of staff on data protection matters related to VIS by the Ministry of Interior (MoI) and Ministry of European and International Affairs (MEIA); the MEIA's multi-pronged approach to auditing the visa process; the information provided by the DPA in regard to the SIS II and VIS is very detailed and readily accessible; the information folders on SIS and VIS on the website of the MoI and that the MoI replies to access requests regarding SIS II or VIS within a short time period.

(3) Recommendations should be made on remedial actions to be taken by Austria in order to address deficiencies identified during the evaluation. In light of the importance of complying with the Schengen *acquis* on personal data protection priority should be given to implementing recommendations 1, 6, 7 and 13 as set out in this Decision.

(4) This Decision should be transmitted to the European Parliament and to the national Parliaments of the Member States. Within three months of its adoption, Austria 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 Austria should:

Legislation

1. implement Article 79 General Data Protection Regulation (GDPR)[1], and transpose Article 54 Directive (EU) 2016/680[2] (LED) into Austrian national law in order to provide for a right to an effective judicial remedy against the decision of a controller or processor that is a public authority;

Data Protection Authority

2. lay down in law the reasons for dismissal of the head and deputy head of the Austrian data protection authority (DPA), in order to avoid the risk of a premature termination of their terms of office other than in a case of serious misconduct or if they no longer fulfil the conditions required for the performance of their duties;

3. ensure that the information technology (IT) expert newly recruited by the DPA and any additional IT expert have or will acquire a comprehensive understanding of the Schengen Information System II (SIS II) and Visa Information System (VIS), as well as of information security management, so that such experts will also be able to be actively involved in the SIS and VIS supervisory activities. Further, the DPA should continue to involve external IT experts in the inspections until it can cover all IT-related inspection tasks by its own staff;

---

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.

4. ensure that the DPA carries out inspection visits to the SIRENE Bureau, inspections of some end user authorities of the system, such as the police, as well as regular checks and analysis of the log files, in order to fulfil its tasks of comprehensively monitoring the processing of SIS II personal data;

5. ensure that the supervisory activities of the DPA in relation to VIS cover also all security aspects, including logs, via regular controls on the basis of log files analysis and that the DPA thoroughly inspects the server rooms and also inspects some other end users of the VIS system, such as the police;

6. ensure that DPA finalises the second audit of the N.VIS as soon as the COVID19 situation allows this;

7. ensure that the DPA carries out an audit of the data processing operations in the N.VIS at least once every four years;

Schengen Information System

8. ensure that all devices allowing access to SIS II data use two-factor authentication;

9. ensure that all documents of the information security management systems in place for both data centres are reviewed more often and that the standards used are still state of the art;

10. ensure that the security plan for SIS II is reviewed on a regular basis and be updated where necessary and that security measures are set to ensure lasting robustness in addition to confidentiality, integrity and accessibility, in particular by ensuring that the controller takes into account the technical development to ensure that the security measures adopted continue to fulfil these aims;

11. clarify whether the Central Clearing Authority is an integral part of the MoI or an external data processor;

12. ensure that for handling cases of misused identities improvements will be made in relation to the information given to the data subject and consent forms used and that the forms given to the data subject include information about data subjects' rights, the contact details of the data protection officer, the legal basis for the processing and information about the period during which the personal data will be stored;

Visa Information System

13. ensure that logs of all data processing operations in the VIS are kept at national level in accordance with Article 34 of the Regulation (EC) 767/2008 (VIS Regulation) (for a period of one year after the retention period referred to in Article 23(1) of the VIS Regulation);

Public Awareness and Rights of Data Subjects

14. ensure that the MoI provides also other (than German) language versions e.g. in English of its website concerning the SIS II and VIS data processing and the related data subjects' rights and makes the information on its website on data subjects' rights in relation to SIS II and VIS data easier accessible;

15. ensure that the MoI provides on its website forms for exercising the rights of access, correction and deletion, both in German and in other languages e.g. in English;

16. make paper versions of the SIS information brochures available and accessible in public authorities;

17. ensure that, in order to enhance the data subjects' rights, the MoI provides an unofficial translation, e.g. in English, of the replies to data subjects;

18. ensure that the websites of Provincial Police Directorates provide information on SIS II and VIS including on related personal data processing and contain links to the website of the DPA;

19. ensure that information on the processing of personal data in the VIS is provided in an easily accessible way on the websites of the MEIA and of consulates and embassies and that those websites contain links to the website of the DPA;

20. ensure that the DPA provides the same information concerning the obligation of the data subject to prove his/her identity on its website (in German and English) as well as in the data subject access request forms;

21. ensure that the DPA provides on its website (in German and English) specific standard forms for rectification and erasure requests in relation to SIS and VIS data;

22. ensure that the DPA provides information on the time limit for lodging a complaint, as specified in Article 24(4) of the DP Act, on the English version of its website.

Done at Brussels,

For the Council
The President