Council of the European Union

Brussels, 4 June 2018
(OR. en)

8850/18

Interinstitutional File: 2018/0051 (NLE)

PARLNAT 108

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 2017 evaluation of Portugal 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 2017 evaluation of Portugal 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.

ANNEX

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2017 evaluation of Portugal 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 Portugal remedial actions to address deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2017. 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(2018)1190].

(2) As a good practice is seen, the on-site team welcomed the Data Protection Authority's continuous investment in training of its technical personnel.

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

(3) In light of the importance to comply with the Schengen acquis, in particular the obligation to ensure and carry out effective supervision and to ensure necessary security measures, priority should be given to implement recommendation(s) 1, 4, 14, 17 and 22 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, Portugal shall, pursuant to Article 16, paragraph 1 of Regulation (EU) No 1053/2013, establish an action plan to remedy the deficiencies identified in the evaluation report and provide this to the Commission and the Council,

HEREBY RECOMMENDS:

that Portugal should

Data Protection Supervisory Authority

1. allocate sufficient financial and human resources to Data Protection Authority (hereinafter "DPA") in order for it to be able to fulfil all tasks entrusted to it under the Schengen Information System II (hereafter "SIS II") and Visa Information System (hereafter "VIS") acquis, also in light of increased responsibilities in future;

2. in order to better ensure the complete independence of DPA, grant the DPA financial autonomy to execute its annual budget and autonomy as regard recruitment of its staff by at minimum aligning the respective rules with those applicable to other independent authorities in Portugal;

3. ensure the DPA finalises the procedure concerning the adoption of the reports following the inspection relating to the processing of the personal data within SIS II without delay;

4. ensure the DPA completes the audit of VIS without delay;

Rights of Data Subjects

5. ensure that data subjects are informed about their rights concerning SIS II on the website of Serviço de Estrangeiros e Fronteiras (Borders and Immigration´s Office, hereinafter "SEF");

6. ensure that the data subject, following their request to access their personal data, are informed about the categories of data actually processed in SIS II;

7. ensure that data subjects are provided with clear information as regards the identity of the data controller for processing of their personal data in the framework of issuing Schengen visas;

Visa Information System

8. clarify the situation concerning the controllership of the processing of personal data in N.VIS (encompassing the applications used both by Ministry of Foreign Affairs (hereafter "MFA") and SEF, and related data centres) in particular by clarifying the role of the MFA and by clarifying the allocation of responsibilities related to processing of personal data between SEF and MFA;

9. ensure that MFA carries out systematic supervisory activities allowing for the meaningful assessment of the aspects related to the processing of personal data by External Service Provider (hereafter "ESP"). In this regard, Portugal is encouraged to extend the questionnaire MFA sends to ESP in order to cover in a more detailed way the data protection aspects and to enhance the supervisory activities of MFA related to data protection carried out by the ESP and the subcontractor, as the case may be;

10. provide for a procedure that allows verification of SIS II hits in the course of the visa procedure;

11. ensure all N.VIS users' passwords are encrypted;

12. ensure that SEF and MFA analyse the log files on a regular basis in order to ensure the data protection monitoring;

13. ensure that MFA performs the self-monitoring of the processing of personal data in the RPV and related data centre on a regular basis;

14. ensure that MFA adopts security plan for the RPV and related data centre without delay;

15. fully implement Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences and ensures that access to N.VIS data respect the requirements and procedure established therein;

16. ensure that ESP deletes personal data of applicants it stores on its systems in line with deadlines of Annex X, part A, point (d), of the Visa Code, requiring such data are deleted immediately after their transmission to the consulate;

Schengen Information System II

17. provide for the full backup site for the N.SIS II which provides full functionalities including the connection with s-Testa communication infrastructure;

18. clarify the responsibilities between the parties involved in processing of N.SIS II data, that is the data controller and the authorities accessing SIS.II (user authorities) in terms of IT security, control and self-monitoring thereof, for example by concluding agreements between the data controller and authorities accessing SIS II;

19. implement a user management that allows for an effective self-monitoring on the basis of central logs by the N.SIS II data controller without the need to consult logs at user authorities;

20. ensure that SEF analyses the log files on a regular basis in order to ensure the data protection monitoring;

21. ensure that IT environments that are used by users with far reaching access or editorial rights to N.SIS II (such as members of the SIRENE Bureau) are logically or physically separated from internet access;

22. ensure that the data controller encrypts the N.SIS backup tapes and hard-disks;

23. ensure that user profiles with far reaching access or editing rights to N.SIS II data (such as members of the SIRENE Bureau) are secured with a mandatory method of two-factor authentication;

24. ensure that SEF enhances its activities related to the self-monitoring of the processing of personal data in N.SIS and performs such self-monitoring on a regular basis; the Portugal is encouraged to allocate sufficient financial and human resources to SEF to ensure effective and continuous self-auditing and IT security in particular by ensuring that the post for the employee for the IT security in SEF's Information technology division is filled in;

Public Awareness

25. ensure that website of SEF provides for the appropriate links to the DPA website.

Done at Brussels,

For the Council
The President