Council of the
European Union

Brussels, 23 March 2018
(OR. en)

7153/18

Interinstitutional File:
2017/0304 (NLE)

PARLNAT 62

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 Denmark 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 Denmark 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 Denmark 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 Denmark 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(2017) 7100].

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

(2) As good practice are seen amongst others that the Danish Immigration Service (hereafter DIS) provides detailed and accessible information on the processing of persona data in the visa issuing procedure and the related data subjects' rights on its website *www.newtodenmark.dk* , that the MFA has issued "Instructions for Danish Missions – Supervision of External Service Provider (ESP)" in which in general terms is described how the mission supervises the ESP including in relation to data protection and data security as well as creation of the Data Protection Unit at the Danish National Police (hereafter DNP) which has the lead on all legal aspects of data protection issues for the DNP and will in future also provide guidance on practical implementation.

(3) In light of the importance to comply with the Schengen acquis, in particular to ensure the lawfulness of processing of personal data in the SIS II and national VIS, priority should be given to implement recommendations 5, 7 and 21.

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

Data Protection Supervisory Authority

1. in order to better ensure the complete independence of the Danish Data Protection Authority (hereafter DPA) adopt the planned formalised rules on the organisation of the DPA which should include more detailed rules on the selection process and terms of appointment of the members of the Council;

2. in order to better ensure the complete independence of the Danish Data Protection Authority (hereafter DPA) reassess the involvement of the Ministry of Justice in the selection and appointment of some of the deputy Directors and its role in selecting the young lawyers;

3. allocate sufficient financial and human resources to the 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;

4. ensure that the DPA strenghtens its monitoring of the lawfulness of the processing of SIS II personal data by carrying out inspections (including the checking of log-files) on a more regular basis;

5. ensure that, at least every four years, audits of data processing operations in N.SIS will be carried out by the DPA; as the deadline for the first audit is April 2017 actions should be taken to fulfil this obligation as soon as possible;

6. ensure that the DPA strenghtens its monitoring of the lawfulness of the processing of VIS personal data by carrying out inspections (including the checking of log-files) on a more regular basis;

7. ensure that, at least every four years, audits of data processing operations in the national system of VIS will be carried out. 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

8. ensure that the information on data subjects' rights in relation to SIS II data on the website of the DNP will be more detailed and easier to access;

9. update the standard form for making an access request in relation to SIS II data which is provided on the websites of the DPA and the Danish National Police (hereafter DNP); provide also standard forms for corrections and deletion requests on the websites of the DPA and the DNP; provide the specific forms also in Danish;

10. provide information on the processing of personal data in the visa issuing procedure including in VIS and on the related data subjects' rights on the website of the DPA;

11. provide specific model letters for VIS data subjects' requests;

Visa Information System

12. ensure through action of the Ministry of Foreign Affairs (hereafter MFA) that all visa application files scanned by the External Service Providers are encrypted before they are being transported to the diplomatic mission;

13. take the necessary steps that the Ministry of Immigration and Integration (hereafter MII) better ensure redundancy of the N-VIS database in order to avoid breakdowns;

14. take the necessary steps that the MFA develops a procedure to ensure a regular revision of the access authorisations provided to users of the UM-VIS database, including their deactivation if necessary;

15. consider whether to add an additional password requirement for access to the software application giving access to the N-VIS database in the DIS;

16. develop a procedure to perform regular and systematic analysis of the log files to detect any possible misuse in the VIS system;

17. take the necessary steps that the MII/DIS and STATENS IT formalise their data controller-processor relationship in a written agreement setting out both bodies' responsibilities, notably on information security and processing of personal data;

18. take the necessary steps that the MII/DIS and MFA formalise their data controller-processor relationship in a written agreement setting out both bodies' responsibilities, notably on information security and processing of personal data;

19. take the necessary steps that the MII finalises clarifying the tasks and responsibilities of the different authorities involved in the visa issuing procedure;

20. ensure that records of processing operations in C-VIS are kept for a period of one year after the retention period referred to in Article 23 (1) of the VIS Regulation (EC) 767/2008 has expired;

21. ensure that the MII including the DIS as well as the MFA adopt security plans for the N-VIS system;

Schengen Information System II

22. ensure that the DNP provides a basic training module for all operational and administrative staff (police officers and civilian staff) specifically on data protection and data security in order to contribute to the lawful processing of SIS II data;

23. ensure that the DNP raises awareness that the information security policy (Informationssikkerhedspolitik) and the IT security manual (It-sikkerhedshåndbog) (which cover all information systems run by the DNP) are also applicable to the N-SIS II;

Public Awareness

24. provide on the English website of the DPA general information on the SIS II, including on processing of personal data in the SIS II;

25. provide on the Danish and English websites of the DPA general information on the VIS;

26. provide on the website of the DNP general information on the SIS II including on processing of personal data in the SIS II;

27. provide printed information for the public on SIS II and VIS, and on data subjects' rights, in the DPA's, DNP's, MII's and DIS's offices.

Done at Brussels,

For the Council
The President