Council of the European Union

Brussels, 25 April 2017
(OR. en)

8465/17

Interinstitutional File:
2017/0052 (NLE)

SCH-EVAL 124
COMIX 295

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	25 April 2017
To:	Delegations
No. prev. doc.:	8047/17
Subject:	Council Implementing Decision setting out a recommendation on addressing the deficiencies identified in the 2015 evaluation of Germany 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 2015 evaluation of Germany on the application of the Schengen *acquis* in the field of data protection, adopted by the Council at its 3531st meeting held on 25 April 2017.

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.

ANNEX

Council Implementing Decision setting out a

RECOMMENDATION

on addressing the deficiencies identified in the 2015 evaluation of Germany on the application of the Schengen acquis in the field of data protection

THE COUNCIL 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 setting out a recommendation is to recommend to Federal Republic of Germany remedial actions to address deficiencies identified during the Schengen evaluation in the field of data protection carried out in 2015. 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)1081].

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

(2) The following is considered a best practice: having legislation in place which requires an "opening order" (*Errichtungsanordnung*) for each automated data file containing personal data, in accordance with section 34 of the Act on the Federal Criminal Police Office and the Cooperation between the Federation and the Länder in Criminal Police Matters (BKAG) and in accordance with the Police Data Protection Acts of some of the federal states (hereafter Länder) with approval requirements and mandatory consultation of the Federal Commissioner for Data Protection and Freedom of Information in line with applicable legislation; the appointment of a mandatory Data Protection Officer in the Federal Criminal Office, the Federal Police and the Länder Police Forces; the possibility to submit multiple data subject access requests free of charge; self-monitoring practices and the review of data processing and security measures undertaken by the Federal Office of Administration and the Federal Foreign Office in accordance with the Visa Information System (hereafter VIS) legal framework; and the internal procedures in the Federal Criminal Police Office (*Bundeskriminalamt)* to ensure the compliance of the security information systems with the relevant technical standards.

(3) In light of the importance to comply with the Schengen acquis, in particular the supervision activities by the competent data protection supervisory authorities as well as by the data processing authorities, priority should be given to implement recommendations 1–4 and 8-13.

(4) This decision setting out a recommendation should be transmitted to the European Parliament and to the parliaments of the Member States. Within three months of its adoption, the evaluated Member State 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 Germany should

Supervision activities by the Federal Commissioner for Data Protection and Freedom of Information and the Data Protection Supervisory Authorities of the Länder

1. implement a system for the supervision and monitoring of Schengen Information System II (hereafter SIS II) activities to be carried out by the Federal Commissioner for Data Protection and Freedom of Information and provide evidence about those activities;

2. implement a system for the SIS II supervision and monitoring activities to be carried out by the Data Protection Supervisory Authorities of the Länder and provide evidence about those activities;

3. implement a system for supervision and monitoring activities of VIS carried out by the Federal Commissioner for Data Protection and Freedom of Information and provide evidence about those activities;

4. ensure that at least every four years audits of the data processing operations in its N.VIS are carried out in accordance with international auditing standards set up in the applicable legal framework for the VIS and provide evidence about those audits;

Access rights

5. take the necessary measures to ensure transparency for individuals, in particular concerning their right to being informed about their requests for access, not later than 60 days from the date on which the request for access was submitted and on the possibility for seeking a judicial remedy in all cases where such information is not provided after 60 days;

Visa Information System and Schengen Information System

6. ensure and provide evidence that visa applicants are informed about the processing and protection of their personal data prior to entering their personal data into the visa application when using the available online forms;

7. determine and formalise the relationship between the Federal Foreign Office and the Federal Office of Administration in terms of data controller, data processor or joint controllers with regard to the national part of the VIS;

8. provide evidence that the Federal Foreign Office carries out regular checks on the content of the logs on the use of SIS II for processing of visa applications;

9. require all public authorities with access to N.SIS II to put in place plans for future checks on the lawfulness of data processing;

10. put in place a system to ensure the accuracy and completeness of the log records of the N.SIS in accordance to the applicable legal framework (integrity of data);

11. implement the recommendations of 2009 and strengthen the authentication mechanism on SIS II, preferably by implementing a two-factor authentication system;

12. review the access rights granted to all National Police Information System (INPOL) users in SIS II and ensure that user profiles are defined strictly according to their need for access;

13. put in place a system according to which the Federal Commissioner for Data Protection and Freedom of Information is notified of any personal data breach in N.SIS II;

14. review the integration of external components in the processing of messaging to ensure full compliance with data retention rules across the SIRENE information process;

15. submit a timetable for the Federal Criminal Police Office, as controller of SIS II, to ensure that log records related to accesses carried out by all authorities with access to SIS II meet the requirements of Article 12(3) of the SIS II Regulation and Decision;

Awareness raising

16. update the information for individuals on exercising their right to the protection of personal data in the framework of data processing in SIS II on the websites of the Federal Commissioner for Data Protection and Freedom of Information, the Federal Criminal Police Office, the Federal Ministry of Interior, the Federal Office of Administration and the Federal Foreign Office.

Done at Brussels,

For the Council
The President