Consejo de la Unión Europea

Bruselas, 14 de mayo de 2018
(OR. en)

8792/18

**Expediente interinstitucional: 2018/0051 (NLE)**

**SCH-EVAL 102**
**COMIX 244**

**RESULTADO DE LOS TRABAJOS**

| | |
|---|---|
| De: | Secretaría General del Consejo |
| Fecha: | 14 de mayo de 2018 |
| A: | Delegaciones |
| N.º doc. prec.: | 8285/18 |
| Asunto: | Decisión de Ejecución del Consejo por la que se formula una Recomendación para subsanar las deficiencias detectadas en la evaluación de 2017 de la aplicación por parte de **Portugal** del acervo de Schengen en materia de **protección de datos** |

Adjunto se remite a las delegaciones la Decisión de Ejecución del Consejo por la que se formula una Recomendación para subsanar las deficiencias detectadas en la evaluación de 2017 relativa a la aplicación por parte de Portugal del acervo de Schengen en materia de protección de datos, adoptada por el Consejo en su sesión celebrada el 14 de mayo de 2018.

De conformidad con el artículo 15, apartado 3, del Reglamento (UE) n.º 1053/2013 del Consejo, de 7 de octubre de 2013, la presente Recomendación se remitirá al Parlamento Europeo y a los Parlamentos nacionales.

**ANEXO**

Decisión de Ejecución del Consejo por la que se formula una

**RECOMENDACIÓN**

**para subsanar las deficiencias detectadas en la evaluación de 2017 de la aplicación por parte de Portugal del acervo de Schengen en materia de protección de datos**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 1053/2013 del Consejo, de 7 de octubre de 2013, por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen, y se deroga la Decisión del Comité Ejecutivo de 16 de septiembre de 1998 relativa a la creación de una Comisión permanente de evaluación y aplicación de Schengen[1], y en particular su artículo 15,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) La finalidad de la presente Decisión es proponer a Portugal medidas correctoras orientadas a subsanar las deficiencias detectadas en la evaluación de Schengen en materia de protección de datos realizada en 2017. Tras la evaluación, se adoptó, mediante la Decisión de Ejecución de la Comisión [C(2018) 1190], un informe que exponía las conclusiones y valoraciones e incluía una lista de las mejores prácticas y las deficiencias detectadas durante la evaluación.

(2) El equipo de visitas *in situ* valoró positivamente la indudable buena práctica de la autoridad de protección de datos consistente en invertir de manera continuada en la formación de su personal técnico.

[1] DO L 295 de 6.11.2013, p. 27.

(3) Teniendo en cuenta hasta qué punto es importante cumplir el acervo de Schengen, en especial, las obligaciones de garantizar y llevar a cabo una supervisión efectiva y de velar por que se adopten las medidas de seguridad necesarias, debe darse prioridad a la aplicación de las recomendaciones 1, 4, 14, 17 y 22.

(4) La presente Decisión deberá transmitirse al Parlamento Europeo y a los Parlamentos de los Estados miembros. En el plazo de tres meses a partir de su adopción, Portugal debe, de conformidad con el artículo 16, apartado 1, del Reglamento (UE) n.º 1053/2013, establecer un plan de acción para subsanar las deficiencias detectadas en el informe de evaluación y presentarlo a la Comisión y al Consejo.

RECOMIENDA:

Portugal debería:

**Autoridad de supervisión de la protección de datos**

1. Asignar suficientes recursos financieros y humanos a la autoridad de protección de datos (en lo sucesivo, «APD») con el fin de que pueda desempeñar todas las tareas que se le han encomendado en el marco del Sistema de Información de Schengen de segunda generación (en lo sucesivo, «SIS II») y del acervo del Sistema de Información de Visados (en lo sucesivo, «VIS»), y en previsión ante un aumento futuro de sus responsabilidades.

2. A fin de garantizar de mejor modo la total independencia de la APD, concederle autonomía financiera para ejecutar su presupuesto anual y autonomía en lo que se refiere a la contratación de su personal, mediante, al menos, la armonización de las normas respectivas con las aplicables a otras autoridades independientes en Portugal.

3. Velar por que la APD finalice sin demora el procedimiento de adopción de los informes correspondientes a la inspección relacionada con el tratamiento de los datos personales en el SIS II.

4. Velar por que la APD complete la auditoría del VIS sin demora.

**Derechos de los interesados**

5. Asegurarse de que el sitio web del Serviço de Estrangeiros e Fronteiras (Servicio de Extranjería y Fronteras; en lo sucesivo, «SEF») informe a los interesados sobre sus derechos en relación con el SIS II.

6. Garantizar que los interesados sean informados, cuando presenten una solicitud de acceso a sus datos personales, sobre las categorías de datos efectivamente tratados en el SIS II.

7. Cerciorarse de que los interesados reciban información clara sobre la identidad del responsable del tratamiento de sus datos personales en el marco de la expedición de visados Schengen.

**Sistema de Información de Visados**

8. Aclarar la situación relativa a la responsabilidad del tratamiento de datos personales en su sistema nacional de información sobre visados (en lo sucesivo, «N.VIS»), que comprende las solicitudes relativas tanto al Ministerio de Asuntos Exteriores (en lo sucesivo, «MAE») y al SEF como a los centros de datos relacionados; en particular, definir el papel del MAE y precisar la asignación de responsabilidades relacionadas con el tratamiento de los datos personales entre el SEF y el MAE.

9. Velar por que el MAE lleve a cabo actividades sistemáticas de supervisión que permitan evaluar de modo significativo los aspectos relacionados con el tratamiento de datos personales por los proveedores de servicios externos (en lo sucesivo, «PSE»); a este respecto, se invita a Portugal a ampliar el cuestionario que el MAE envía a los PSE para abarcar de forma más detallada la cuestión de la protección de los datos y para mejorar las actividades de supervisión del MAE relativas a la protección de datos llevada a cabo por los PSE y, en su caso, los subcontratistas.

10. Establecer el procedimiento para verificar las respuestas positivas del SIS II en el curso de procedimientos de expedición de visados.

11. Garantizar que las contraseñas de todos los usuarios del N.VIS estén cifradas.

12. Velar por que el SEF y el MAE analicen los archivos de registro periódicamente con el fin de garantizar la supervisión de la protección de datos.

13. Velar por que el MAE lleve a cabo un seguimiento interno periódico del tratamiento de los datos personales en la Rede de Pedidos de Visto (RPV; red de solicitudes de visado) y en los centros de datos relacionados.

14. Velar por que el MAE adopte sin demora un plan de seguridad para la RPV y los centros de datos relacionados.

15. Aplicar en su integridad la Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, y garantizar que el acceso a los datos del N.VIS respete el procedimiento y los requisitos que dicha Decisión establece.

16. Velar por que los PSE supriman los datos personales de los solicitantes que almacenen en sus sistemas inmediatamente después de su transmisión al consulado, de conformidad con el anexo X, parte A, letra d), del Código de visados.

**Sistema de Información de Schengen II**

17. Acondicionar la instalación de seguridad completa (full backup site) del N.SIS II, que deberá ofrecer todas las funcionalidades, incluida la conexión con la infraestructura de comunicación s-TESTA.

18. Delimitar las responsabilidades de las partes implicadas en el tratamiento de datos del N.SIS II, a saber, el responsable del tratamiento de los datos y las autoridades que acceden al SIS II (autoridades usuarias), en términos de seguridad informática, control y seguimiento interno; por ejemplo, mediante la conclusión de acuerdos entre dichas partes.

19. Poner en marcha un sistema de gestión de usuarios que permita hacer un seguimiento interno eficaz basado en los registros centrales del responsable del tratamiento de datos del N.SIS II sin que sea preciso consultar los registros de las autoridades usuarias.

20. Velar por que el SEF analice los archivos de registro de forma periódica para garantizar la supervisión de la protección de datos.

21. Garantizar que los entornos informáticos que sean utilizados por usuarios con derechos de acceso o de edición amplios en el N.SIS II (como los miembros de la Oficina Sirene) estén virtual o físicamente aislados de internet.

22. Asegurarse de que el responsable del tratamiento de datos cifre los discos duros y cintas de seguridad del N.SIS.

23. Asegurarse de que los perfiles de usuario con derechos de acceso o de edición amplios en el N.SIS II (como los miembros de la Oficina Sirene) estén protegidos con un sistema obligatorio de autenticación bifactorial.

24. Velar por que el SEF refuerce sus actividades relacionadas con el seguimiento interno del tratamiento de datos personales en el N.SIS y realice dicho seguimiento de forma periódica; en este sentido, se invita a Portugal a asignar recursos humanos y financieros suficientes al SEF para garantizar un sistema eficaz e ininterrumpido de seguridad informática y auditorías internas, en particular, velando por que el puesto de encargado de la seguridad informática en el departamento de informática del SEF esté cubierto.

**Sensibilización de la opinión pública**

25. Garantizar que en el sitio web del SEF figuren los enlaces correspondientes al sitio web de la APD.

Hecho en Bruselas, el

*Por el Consejo*
*El Presidente*