Consejo de la Unión Europea

Bruselas, 17 de junio de 2022
(OR. en)

10396/22

Expediente interinstitucional: 2021/0224(NLE)

SCH-EVAL 83
DATAPROTECT 197
COMIX 324

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	17 de junio de 2022
A:	Delegaciones
N.º doc. prec.:	7788/22
Asunto:	Decisión de Ejecución del Consejo por la que se formula una recomendación para subsanar las deficiencias detectadas en la evaluación de 2020 relativa a la aplicación por parte de **Austria** 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 2020 relativa a la aplicación por Austria del acervo de Schengen en materia de protección de datos, aprobado por el Consejo el 17 de junio de 2022.

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

Decisión de Ejecución del Consejo por la que se formula una

RECOMENDACIÓN

para subsanar las deficiencias detectadas en la evaluación de 2020 relativa a la aplicación por parte de Austria 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) En noviembre de 2020 se llevó a cabo una evaluación de Schengen en el ámbito de la protección de datos en relación con Austria. Tras la evaluación se adoptó, mediante la Decisión de Ejecución C(2021) 9200 de la Comisión, un informe en el que se exponen las conclusiones y valoraciones y se incluye una lista de las mejores prácticas y las deficiencias detectadas durante la evaluación.

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

(2) Se consideran buenas prácticas, en particular, las siguientes: que, desde la última evaluación, el personal de la autoridad austriaca de protección de datos (APD) se haya visto y vaya a seguir viéndose reforzado, en paralelo a un aumento del presupuesto; que los acuerdos entre responsables y encargados del tratamiento en relación con los datos del VIS ofrezcan un elevado nivel de protección de datos y garanticen que todas las partes implicadas en el tratamiento de datos del VIS dispongan de las salvaguardias pertinentes en materia de protección de datos; que, tanto desde el Ministerio del Interior como desde el Ministerio de Asuntos Europeos e Internacionales, se esté impartiendo formación al personal sobre cuestiones de protección de datos relacionadas con el VIS; el enfoque multifacético del Ministerio de Asuntos Europeos e Internacionales a la hora de auditar el proceso de expedición de visados; que la información facilitada por la APD en relación con el SIS II y el VIS sea muy detallada y fácilmente accesible; que la documentación sobre el SIS y el VIS se recoja en el sitio web del Ministerio del Interior y que este responda a las solicitudes de acceso al SIS II o al VIS en un plazo breve.

(3) Deben formularse recomendaciones sobre las medidas correctoras que debe adoptar Austria para subsanar las deficiencias detectadas durante la evaluación En vista de la importancia de cumplir el acervo de Schengen en materia de protección de datos personales, debe darse prioridad a la aplicación de las recomendaciones 1, 6, 7 y 13 formuladas en la presente Decisión.

(4) La presente Decisión debe transmitirse al Parlamento Europeo y a los Parlamentos de los Estados miembros. En el plazo de tres meses desde su adopción, Austria debe establecer, con arreglo al artículo 16, apartado 1, del Reglamento (UE) n.º 1053/2013, un plan de acción en el que figuren todas las recomendaciones dirigidas a subsanar cualquier deficiencia detectada en el informe de evaluación, y presentarlo a la Comisión y al Consejo.

RECOMIENDA:

que Austria debería:

Legislación

1. aplicar el artículo 79 del Reglamento general de protección de datos (RGPD)[1] y transponer el artículo 54 de la Directiva (UE) 2016/680[2] al Derecho nacional austriaco con el fin de establecer el derecho a la tutela judicial efectiva contra la decisión de un responsable o encargado del tratamiento que sea una autoridad pública;

Autoridad de protección de datos

2. establecer legalmente las razones de la destitución del jefe y del jefe adjunto de la autoridad austriaca de protección de datos (APD), con el fin de evitar el riesgo de cese anticipado de sus mandatos, solo aceptable en caso de falta grave o si ya no cumplen las condiciones requeridas para el ejercicio de sus funciones;

3. garantizar que tanto los expertos en tecnologías de la información (TI) recientemente contratados por la APD como cualquier otro experto en TI tengan o adquieran una comprensión completa del Sistema de Información de Schengen II (SIS II) y del Sistema de Información de Visados (VIS), así como de la gestión de la seguridad de la información, de modo que tales expertos también puedan participar activamente en las actividades de supervisión del SIS y del VIS; además, la APD debe seguir implicando a expertos en TI externos en las inspecciones hasta que pueda cubrir todas las tareas de inspección relacionadas con las TI con su propio personal;

---

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

[2] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

4. garantizar que la APD organice visitas de inspección a la oficina Sirene, y realice inspecciones de algunas de las autoridades que sean usuarios finales del sistema, como la policía, así como controles y análisis periódicos de los archivos de registro, para cumplir así sus tareas de supervisión exhaustiva del tratamiento de los datos personales del SIS II;

5. garantizar que las actividades de supervisión de la APD en relación con el VIS incluyan también todos los aspectos de seguridad, incluidos los registros, mediante controles periódicos basados en el análisis de los archivos de registro, y que la APD inspeccione exhaustivamente las salas de servidores e inspeccione igualmente a otros usuarios finales del sistema VIS, como la policía;

6. garantizar que la APD concluya la segunda auditoría del N.VIS tan pronto como lo permita la situación de la COVID-19;

7. garantizar que la APD lleve a cabo una auditoría de las operaciones de tratamiento de datos en el N.VIS al menos una vez cada cuatro años;

Sistema de Información de Schengen

8. garantizar que todos los dispositivos que permiten acceder a los datos del SIS II utilicen una autenticación bifactorial;

9. garantizar que todos los documentos de los sistemas de gestión de la seguridad de la información existentes para ambos centros de datos se revisen con mayor frecuencia y que las normas utilizadas sigan siendo las más avanzadas;

10. garantizar que el plan de seguridad para el SIS II se revise periódicamente y se actualice cuando sea necesario, y que se establezcan medidas de seguridad para garantizar una eficacia duradera, además de la confidencialidad, integridad y accesibilidad necesarias, en particular velando por que el responsable del tratamiento tenga en cuenta el desarrollo técnico para asegurarse de que las medidas de seguridad adoptadas sigan cumpliendo estos objetivos;

11. aclarar si la Autoridad Central de Validación (Zentrale Clearingstelle) es parte integrante del Ministerio del Interior o un encargado externo de tratamiento de datos;

12. garantizar que, para tratar los casos de identidades utilizadas indebidamente, se introduzcan mejoras en relación con la información facilitada al interesado y los formularios de consentimiento utilizados, y que los formularios facilitados al interesado incluyan información sobre los derechos de los interesados, los datos de contacto del delegado de protección de datos, la base jurídica para el tratamiento y la información sobre el período durante el cual se conservarán los datos personales;

Sistema de información de visados

13. garantizar que los registros de todas las operaciones de tratamiento de datos en el VIS se conserven a nivel nacional de conformidad con el artículo 34 del Reglamento (CE) n.º 767/2008 (Reglamento VIS) (durante un período de un año tras el período de conservación a que se refiere el artículo 23, apartado 1, del Reglamento VIS);

Sensibilización pública y derechos de los interesados

14. garantizar que el Ministerio del Interior también ofrezca otras versiones lingüísticas (distintas del alemán), por ejemplo, en inglés, de su sitio web en lo referente al tratamiento de datos del SIS II y del VIS y a los correspondientes derechos de los interesados, y facilite en mayor medida el acceso a la información que figura en su sitio web sobre los derechos de los interesados en relación con los datos del SIS II y del VIS;

15. garantizar que el Ministerio del Interior facilite en su sitio web formularios para el ejercicio de los derechos de acceso, rectificación y supresión, tanto en alemán como en otras lenguas, por ejemplo, en inglés;

16. poner a disposición de las autoridades públicas versiones en papel de los folletos informativos del SIS, facilitando el acceso a ellas;

17. garantizar que, con el fin de reforzar los derechos de los interesados, el Ministerio del Interior facilite una traducción no oficial, por ejemplo, en inglés, de las respuestas a los interesados;

18. garantizar que los sitios web de las direcciones provinciales de policía proporcionen información sobre el SIS II y el VIS, en particular por lo que se refiere al tratamiento de datos personales correspondiente, y contengan enlaces al sitio web de la APD;

19. garantizar que la información sobre el tratamiento de datos personales en el VIS se facilite de forma fácilmente accesible en los sitios web del Ministerio de Asuntos Europeos e Internacionales y de los consulados y embajadas, y que estos sitios web contengan enlaces al sitio web de la APD;

20. garantizar que la APD facilite la misma información sobre la obligación del interesado de demostrar su identidad en su sitio web (en alemán e inglés), así como en los formularios de solicitud de acceso del interesado;

21. garantizar que la APD facilite en su sitio web (en alemán e inglés) formularios normalizados específicos para las solicitudes de rectificación y supresión en relación con los datos del SIS y del VIS;

22. garantizar que la APD facilite información sobre el plazo para presentar una reclamación, tal como se especifica en el artículo 24, apartado 4, de la Ley de protección de datos, en la versión inglesa de su sitio web.

Hecho en Bruselas, el

Por el Consejo
El Presidente / La Presidenta