Consejo de la Unión Europea

Bruselas, 14 de mayo de 2025
(OR. en)

8833/25

Expediente interinstitucional:
2024/0126(NLE)

SCH-EVAL 29
DATAPROTECT 88
COMIX 140
NO
CH
IS
LI

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
N.º doc. prec.:	8093/25
Asunto:	Decisión de Ejecución del Consejo por la que se formula una recomendación para subsanar las deficiencias detectadas en la evaluación de 2021 relativa a la aplicación por parte de Italia del acervo de Schengen en el ámbito de la 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 2021 relativa a la aplicación por parte de Italia del acervo de Schengen en el ámbito de la protección de datos, adoptada por el Consejo en su sesión del 12 de mayo de 2025.

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.

ANEXO

Decisión de Ejecución del Consejo por la que se formula una

RECOMENDACIÓN

para subsanar las deficiencias detectadas en la evaluación de 2021 relativa a la aplicación por parte de Italia del acervo de Schengen en el ámbito de la 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, apartado 3,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) En septiembre de 2021 se llevó a cabo una evaluación de Schengen en el ámbito de la protección de datos personales con respecto a Italia. Tras la evaluación, se adoptó, mediante la Decisión de Ejecución C(2024) 1910 de la Comisión, de 30 de mayo de 2024, un informe en el que se exponen las conclusiones y valoraciones y se incluye una lista de las buenas 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 amplias medidas de seguridad relativas a la seguridad física del servidor del Sistema Nacional de Información de Schengen (N.SIS); la completa formación impartida al personal del N.SIS y de la Oficina SIRENE y a los usuarios finales, especialmente en lo que respecta a los esfuerzos de formación y concienciación realizados por la oficina del delegado de protección de datos; los amplios esfuerzos de la oficina del delegado para mejorar la protección y la seguridad de los datos, también para el N.SIS; las inspecciones periódicas llevadas a cabo por el Ministerio de Asuntos Exteriores y Cooperación Internacional (MAECI) en las embajadas y consulados, así como la inspección a los proveedores de servicios externos por parte de las embajadas y consulados sobre la base del documento de orientación del MAECI; los carteles en el aeropuerto y en la comisaría de policía, que facilitan el acceso a la información sobre el SIS a través de códigos QR en múltiples lenguas; la información sobre los derechos de los interesados en el Sistema de Información de Schengen (SIS) facilitada en los sitios web de la Polizia di Stato (Policía estatal) y de la autoridad de protección de datos (APD), que es útil y accesible; que el sitio web del Ministerio del Interior incluya enlaces a la página de inicio de la Polizia di Stato, que ofrece a los interesados una forma fácil y rápida de ejercer sus derechos; que la Polizia di Stato informe a los interesados si sus datos no figuran en el SIS; la información sobre los derechos de los interesados en el Sistema de Información de Visados (VIS) facilitada en el sitio web de la APD, que es útil y accesible.

(3) Deben formularse recomendaciones sobre las medidas correctoras que ha de adoptar Italia para subsanar las deficiencias detectadas en la evaluación. Habida cuenta de la importancia que reviste el cumplimiento del acervo de Schengen en el ámbito de la protección de datos personales y, en particular, por lo que concierne a la supervisión por parte de la autoridad de protección de datos y a la formación relativa al SIS y al VIS, debe darse prioridad a la aplicación de las recomendaciones 4 y 6 establecidas en la presente Decisión.

(4) De conformidad con el artículo 15, apartado 3, del Reglamento (UE) n.º 1053/2013, el Consejo debe remitir la presente Decisión al Parlamento Europeo y a los Parlamentos nacionales de los Estados miembros.

(5) El Reglamento (UE) 2022/922[2] del Consejo es aplicable a partir del 1 de octubre de 2022. Según lo dispuesto en su artículo 31, apartado 3, las actividades de vigilancia y seguimiento de los informes de evaluación y las recomendaciones, empezando por la presentación de los planes de acción, deben llevarse a cabo de conformidad con dicho Reglamento.

(6) En el plazo de dos meses desde la adopción de la presente Decisión, Italia debe establecer, de conformidad con el artículo 21, apartado 1, del Reglamento (UE) 2022/922 del Consejo, un plan de acción para aplicar todas las recomendaciones y subsanar cualquier deficiencia detectada en el informe de evaluación. Italia debe presentar dicho plan de acción a la Comisión y al Consejo.

---

[2] Reglamento (UE) 2022/922 del Consejo, de 9 de junio de 2022, relativo al establecimiento y el funcionamiento de un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen, y por el que se deroga el Reglamento (UE) n.º 1053/2013 (DO L 160 de 15.6.2022, p. 1).

RECOMIENDA:

que Italia, con respecto a:

la autoridad de protección de datos (APD)

1. garantice que la APD participe formalmente en el procedimiento presupuestario, en particular, que tenga una influencia formal en la propuesta de su propio presupuesto antes de que el proyecto de presupuesto general se envíe al Parlamento para su debate y aprobación;

2. garantice que se asigne a la APD suficiente personal para llevar a cabo la supervisión del SIS y del VIS de manera oportuna y eficaz;

3. lleve a cabo inspecciones periódicas de algunas autoridades usuarias finales del sistema, como las autoridades policiales operativas, que incluyan controles y análisis periódicos de los archivos de registro, a fin de que la APD pueda desempeñar sus funciones de supervisión exhaustiva del tratamiento de datos personales en el SIS;

4. finalice la auditoría pendiente de las operaciones de tratamiento de datos en el N.SIS tan pronto como la situación de la COVID-19 lo permita y garantice que se lleven a cabo las siguientes auditorías dentro del período de cuatro años preceptivo;

5. garantice que también se inspeccione periódicamente a más autoridades usuarias finales del sistema VIS, como la policía, la guardia de fronteras y las autoridades de inmigración, con el fin de que la APD pueda desempeñar sus funciones de supervisión exhaustiva del tratamiento de datos personales en el VIS;

6. garantice que las auditorías del sistema nacional de visados se lleven a cabo dentro del período preceptivo de cuatro años;

7. garantice que las auditorías del VIS incluyan también al Ministerio del Interior, como segundo responsable del tratamiento del VIS, además de las medidas de auditoría del MAECI;

el Sistema de información Schengen

8. garantice que comience a funcionar el emplazamiento separado de recuperación en caso de catástrofe, situado en Bari;

9. garantice que la copia de seguridad de los archivos de registro del N.SIS se conserve fuera de la instalación principal, en una ubicación geográfica distinta de Roma, no solo de forma sistemática, sino a intervalos cortos oportunos entre la realización de las copias;

10. garantice que los sistemas operativos de algunas estaciones de trabajo, como en la Oficina SIRENE y en la comisaría de policía local del Commissariato Trevi-Campo Marzio, se actualicen lo antes posible;

11. garantice que, para el control de los archivos de registro del SIS, se adopten directrices con criterios aplicables a todo el personal de supervisión y se utilice un módulo de *software* para los propios análisis de los archivos de registro del SIS con un sistema de alerta automática para las consultas inusuales, con el fin de detectar usos indebidos;

12. garantice un nivel de seguridad más elevado en relación con el acceso a las bases de datos, como la aplicación SIS, mediante un sistema de autenticación bifactorial;

13. garantice que la APD y el Ministerio del Interior elaboren un documento de entendimiento común o un protocolo sobre los criterios o el umbral para la notificación de las violaciones de la seguridad de los datos del N.SIS a la APD;

14. vuelva a evaluar y aplique las normas de la política de grupo relativa a los bloqueos automáticos en relación con los sistemas informáticos en caso de inactividad en cada estación de trabajo con acceso al SIS;

15. establezca una política de seguridad y protección de datos y supervise las prácticas relativas a la conservación de los datos personales del registro de alojamientos en una base de datos policial para disponer que, una vez conservados todos los datos personales para los controles necesarios en el período inicial, mediante la revisión periódica se garantice que, durante el período máximo de conservación, los datos personales permanezcan almacenados en una base de datos policial tan solo durante el tiempo que sea necesario y proporcionado para los fines del artículo 45 del Convenio de Schengen[3];

el Sistema de Información de Visados (VIS)

16. establezca un límite razonable de intentos fallidos de conexión, teniendo en cuenta errores de tecleo, mala memoria, etc., sobre cuya base el sistema debe bloquear el acceso del usuario al Sistema Nacional de Información de Visados (N.VIS);

17. aplique medidas adicionales para supervisar las autorizaciones de acceso al N.VIS (además de que los usuarios del N.VIS estén sujetos a una revisión estricta y periódica de sus autorizaciones de acceso por parte de la oficina a la que pertenecen), a fin de garantizar la eficacia y la eficiencia del proceso de revisión, por ejemplo, la suspensión automática de la autorización de acceso tras un período de tiempo largo y atípico sin ninguna actividad en el sistema VIS;

18. proporcione un nivel de seguridad superior combinando la lectura de la tarjeta con la inserción de un código PIN personal en los dos lectores RFID instalados en la entrada de la zona del centro de datos del MAECI y en la sala de servidores del VIS;

---

[3] Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes (DO L 239 de 22.9.2000, p. 19).

19. aplique al equipo almacenado en armarios cerrados con llave el mismo criterio ya adoptado para otro equipo de la sala de servidores del N.VIS;

20. aplique un sistema de seguridad adecuado, capaz de facilitar la autenticación de acceso a la sala y la auditoría de eventos, e instale además en la sala de servidores de respaldo del sistema VIS un sistema de extinción de incendios para el equipo eléctrico, como el instalado en la sala de servidores del VIS;

21. instale una infraestructura de recuperación en caso de catástrofe en una ubicación geográfica diferente a la del edificio Farnesina;

22. revise los procesos de copia de seguridad aplicados en las embajadas y consulados, evitando el uso de llaves USB o, en caso de utilizarlas, cifrando la información almacenada;

23. aplique un control automático de los registros del I-VIS;

24. añada un módulo de protección de datos personales al curso de formación interna previo a la incorporación del personal encargado de la expedición de visados;

25. garantice que el MAECI evalúe los aspectos críticos de las listas de alerta locales destacados por la APD, no solo a nivel nacional, sino también manteniendo contactos con los demás consulados implicados, e informe a la APD a su debido tiempo sobre las medidas que pueden adoptarse para garantizar el pleno cumplimiento de los requisitos de protección de datos personales;

26. refuerce la oficina del delegado de protección de datos del MAECI;

la concienciación de la población y los derechos de los interesados

27. garantice que la información sobre el SIS que figura en el sitio web del Ministerio del Interior también sea comprensible para quienes no hablan italiano;

28. garantice que se faciliten en los sitios web de la APD los modelos de cartas en relación con el SIS y que se haga más visible el botón «El nuevo mecanismo para ejercer los derechos de protección de datos» del sitio web pertinente;

29. modifique la respuesta estándar que dice «El interesado no tiene prohibiciones de entrada en el territorio Schengen» (n.º 6), que se considera engañosa en los casos en que no se facilita información sobre la descripción al interesado, por ejemplo, debido a amenazas para la seguridad pública o nacional;

30. garantice que los sitios web del MAECI y del Ministerio del Interior proporcionen un modelo específico para la solicitud de acceso a los datos personales tratados en el VIS;

31. considere la posibilidad de facilitar información sobre el VIS y los derechos de los interesados en relación con el tratamiento de datos personales en el VIS en los pasos fronterizos, como los aeropuertos, de la misma manera que ya se hace para el SIS, por ejemplo, a través de carteles, códigos QR con enlace a más información, etc.

Hecho en Bruselas, el

Por el Consejo
La Presidenta / El Presidente