Consejo de la Unión Europea

Bruselas, 25 de enero de 2021
(OR. en)

5534/21

Expediente interinstitucional: 2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
N.º doc. prec.:	14250/20
Asunto:	Decisión de Ejecución del Consejo por la que se formula una Recomendación para subsanar las deficiencias detectadas en la evaluación de 2019 relativa a la aplicación por **Eslovaquia** 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 2019 relativa a la aplicación por Eslovaquia del acervo de Schengen en materia de protección de datos, aprobada mediante procedimiento escrito el 21 de enero de 2021.

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 2019 relativa a la aplicación por Eslovaquia 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 consiste en recomendar a la República Eslovaca medidas correctoras para subsanar las deficiencias detectadas durante la evaluación de Schengen en materia de protección de datos llevada a cabo en 2019. Tras la evaluación, se adoptó, mediante la Decisión de Ejecución C (2020) 8160 de la Comisión, un informe en el que se exponen las conclusiones y valoraciones y se enumeran las mejores prácticas y deficiencias detectadas durante la evaluación.

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

(2) Entre las buenas prácticas observadas figuran las siguientes: que, desde la última evaluación de Schengen en 2012, la Autoridad de Protección de Datos (APD) haya llevado a cabo de manera periódica actividades de supervisión del SIS II con arreglo a una planificación anual y se haya elaborado un concepto para las inspecciones del SIS II para los próximos cuatro años; que la APD haya llevado a cabo un número considerable de inspecciones del VIS en los consulados; los esfuerzos realizados por la APD y el Ministerio del Interior (MI) para proporcionar información a los titulares de los datos en soporte electrónico e impreso; que existan versiones multilingües de la información sobre temas relacionados con Schengen en el sitio web de la APD y en los folletos; que la APD facilite modelos para las solicitudes de los titulares de los datos del SIS y del VIS; que la oficina Sirene prevea que las respuestas a las solicitudes se hagan no solo en lengua eslovaca, sino también en inglés; que las autoridades eslovacas informen a los titulares de los datos si no se han almacenado datos sobre ellos en el SIS II; que la Sección de Inspección de la Oficina de Inspección del MI lleve a cabo un control muy activo de los registros del VIS y del SIS II; que los dos miembros del Departamento de Seguridad del Ministerio de Asuntos Exteriores y Europeos (MAEE) encargados de las cuestiones relativas a la protección de datos desempeñen un papel muy activo; que el MAEE ofrezca formación en materia de protección de datos a su personal, en particular antes de que se le asigne temporalmente a tareas consulares, y que el Departamento de Seguridad (en su calidad de responsable de la protección de datos) dispense esta formación; que el nivel de seguridad física y de procedimiento establecido para proteger los datos del SIS II sea elevado; que el DPD y el DPD adjunto del Departamento de Protección de Datos de la Sección de Inspección del Servicio de Inspección del MI desempeñen un papel muy activo, especialmente en materia de orientación y de control de los registros del SIS II; que el MI proporcione formación sobre protección de datos a todos los usuarios finales del N.SIS II.

(3) En vista de la importancia que reviste cumplir el acervo de Schengen en materia de protección de datos en relación con el VIS, debe darse prioridad a la aplicación de las recomendaciones 7 y 24.

(4) La presente Decisión debe transmitirse al Parlamento Europeo y a los parlamentos de los Estados miembros. En el plazo de tres meses a partir de su adopción, la República Eslovaca debe, de conformidad con lo dispuesto en el artículo 16, apartado 1, del Reglamento (UE) n.º 1053/2013, establecer un plan de acción en el que figuren todas las recomendaciones dirigidas a subsanar cualquier deficiencia señalada en el informe de evaluación, y presentar dicho plan de acción a la Comisión y al Consejo.

RECOMIENDA:

la República Eslovaca debe:

Autoridad de protección de datos

1. velar por que se siga incrementando el presupuesto y el personal de la APD, con el fin de reforzar el rendimiento y la eficacia de la APD;

2. asegurarse de que la parte del presupuesto general del Estado prevista para la APD sea claramente visible a fin de garantizar que la APD cuente con un presupuesto anual público específico;

3. velar por que, en el procedimiento presupuestario, el Consejo Nacional tenga conocimiento de la posición de la APD sobre sus necesidades presupuestarias y de los debates entre la APD y el Ministerio de Hacienda (MH) sobre el presupuesto;

4. adoptar medidas para que el MH no pueda establecer ninguna correlación entre el presupuesto y el importe de las multas que deba recaudar la APD, ya que esto podría repercutir en la naturaleza y priorización del trabajo de la APD y, por lo tanto, afectar a su independencia. Debe garantizarse que el presupuesto de la APD no pueda reducirse durante el año civil en caso de que la APD no haya recaudado la totalidad del importe estimado de las multas;

5. garantizar que todas las funciones y poderes atribuidos a las autoridades de protección de datos en los artículos 57 y 58 del RGPD se confieran a la APD;

6. garantizar que, además de las actividades de supervisión normales llevadas a cabo por la oficina del N.SIS y la oficina Sirene, la APD supervise a un mayor número de autoridades usuarias finales con acceso al SIS II;

7. garantizar que las actividades de supervisión de la APD en relación con el VIS incluyan la inspección de la Autoridad Central de Visados (ACV) respecto de las operaciones de tratamiento de datos en el N.VIS. Dado que el plazo para la primera auditoría del sistema nacional de visados era octubre de 2015, la APD debería llevar a cabo lo antes posible esta parte de la auditoría que aún no se ha realizado;

8. garantizar que la APD inspeccione también periódicamente a los prestatarios de servicios externos;

Derechos de los titulares de los datos

9. encontrar un medio adecuado para que la APD, el MI y el MAEE informen a los titulares de los datos sobre los riesgos potenciales de presentar copias de documentos de identidad y de información sensible a través de una internet abierta. Se invita al MI y al MAEE a que consideren la posibilidad de ofrecer a los titulares de los datos un canal de transmisión electrónica seguro para la presentación de dichos documentos;

10. garantizar que se respete el plazo de sesenta días para responder a las solicitudes de los titulares de datos del SIS II establecido en el artículo 41, apartado 6, del Reglamento SIS II y en el artículo 58, apartado 6, de la Decisión SIS II, hasta que sea plenamente aplicable (a más tardar el 28 de diciembre de 2021) el nuevo acervo SIS[1], en el que figuran referencias cruzadas al plazo de respuesta a las solicitudes de los titulares de los datos previsto en el RGPD (treinta días con posibilidad de prórroga de otros dos meses cuando sea necesario);

11. considerar la posibilidad de proporcionar una parte de la información impresa (folletos/letreros, etc.) destinada a los titulares de los datos en los locales de las comisarías, así como hacerla visible y fácilmente accesible;

12. considerar la posibilidad de proporcionar, por ejemplo, una versión no oficial en inglés de las decisiones de la APD relativas a las reclamaciones presentadas por los titulares de datos del SIS II; esto ayudaría a los interesados a entender mejor la decisión y reforzaría los derechos de los titulares de los datos;

13. garantizar que la información relativa a los derechos de los titulares de los datos del VIS sea más fácil de encontrar en el sitio web del MAEE; el sitio web también debería proporcionar los modelos para que los titulares de datos del VIS ejerzan sus derechos;

---

[1] Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión, DO L 312 de 7.12.2018, p. 56 (véanse en particular los artículos 66 a 71); Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14) (véanse en particular los artículos 51 a 57).

14. garantizar que el impreso de solicitud de visado contenga información clara sobre las distintas autoridades que tratan datos personales como parte del sistema nacional de visados. En particular, debe informarse de que el MAEE es el responsable del tratamiento de los datos;

15. proporcionar información física (folletos/letreros, etc.) a los titulares de los datos del VIS en las instalaciones de los aeropuertos y otros puntos de control fronterizo, y hacerla visible y fácilmente accesible;

16. garantizar que las respuestas a los titulares de datos en relación con sus datos personales del VIS proporcionen información sobre la posibilidad de presentar un recurso contra la respuesta recibida ante la APD y el tribunal competente;

17. adoptar las medidas necesarias para clarificar las responsabilidades del MAEE y la ACV (MI) en la tramitación de las solicitudes presentadas por los titulares de los datos del VIS y formular orientaciones internas o metodológicas para ambas entidades; esta información debería estar disponible para los titulares de los datos;

Sistema de Información de Visados

18. adoptar las medidas necesarias para aumentar el nivel de seguridad para acceder al entorno de la administración estatal y, en particular, a las solicitudes de visado nacionales en el MAEE y el MI (ACV), en particular mediante el acceso a las bases de datos nacionales de visados por medio de tecnología multifactorial;

19. adoptar las medidas necesarias para mejorar la seguridad física y organizativa en el centro de datos del N.VIS del MAEE, en particular con respecto a los siguientes aspectos:

    – la existencia de un registro en la entrada del centro de datos para el personal informático, los visitantes o los proveedores, cuyo acceso debe ser limitado;

    – la instalación de un sistema de extinción de incendios con gas (aragonito);

    – la instalación de un sistema de detección de fugas de agua;

    – el mantenimiento de suelos sin polvo y ordenados;

    – el cierre de la valla de protección de los servidores de la UE;

20. acelerar el procedimiento de creación de un nuevo centro de datos del N.VIS en otra ubicación y del traslado del centro de datos;

21. considerar la posibilidad de modificar el plazo de conservación local de los ficheros históricos del N.VIS en las misiones diplomáticas y consulares, fijando un plazo en lugar de la cantidad de megaoctetos;

22. considerar la posibilidad de utilizar sistemas automáticos de control de los registros en el MAEE;

23. adoptar las medidas necesarias para que las misiones diplomáticas o el MAEE inspeccionen periódicamente a los prestatarios de servicios externos;

24. adoptar las medidas necesarias para proporcionar formación en materia de protección de datos al personal consular local de forma más sistemática y uniforme;

25. garantizar que la solicitud de visado electrónica contenga la misma información que el formulario de solicitud de visado impreso (tal como se establece en el anexo I del Código de visados de la UE[1]);

Sistema de Información de Schengen II

26. adoptar las medidas necesarias para mejorar el nivel de seguridad del acceso al N.SIS II, en particular utilizando la autenticación multifactorial y solo conexiones HTTPS para acceder al N.SIS II;

27. garantizar que el MI informe a la APD sobre cualquier violación de la seguridad de los datos que pueda entrañar un riesgo para los derechos y libertades de las personas físicas. Además, el MI debería crear un registro de las violaciones de la seguridad de los datos personales;

---

1 Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados). DO L 243 de 15.9.2009, p. 1.

Sensibilización pública

28. considerar la posibilidad de poner los folletos de la APD a disposición de los titulares de los datos en lugares más accesibles, como comisarías de policía, zonas de control fronterizo y sedes consulares;

29. considerar la posibilidad de que las presentaciones, seminarios y actos de puertas abiertas de la APD también sean accesibles al público en general, en particular a los titulares de los datos, dado que les interesa la información sobre el SIS II y el VIS.

Hecho en Bruselas, el

Por el Consejo
El Presidente / La Presidenta