Consejo de la Unión Europea

Bruselas, 24 de septiembre de 2019
(OR. en)

12468/19

Expediente interinstitucional: 2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	20 de septiembre de 2019
A:	Delegaciones
N.º doc. prec.:	11904/19
Asunto:	Proyecto de Decisión de Ejecución del Consejo por la que se formula una recomendación para subsanar las deficiencias detectadas en la evaluación de 2018 relativa a la aplicación por parte de **Lituania** 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 2018 relativa a la aplicación por parte de Lituania del acervo de Schengen en materia de protección de datos, adoptada por el Consejo en su sesión del 20 de septiembre de 2019.

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 2018 relativa a la aplicación por parte de Lituania 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 recomendar a Lituania medidas correctoras orientadas a subsanar las deficiencias detectadas en la evaluación de Schengen en el ámbito de la protección de datos realizada en 2018. Tras la evaluación, se adoptó, mediante la Decisión de Ejecución C(2019) 5700 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, entre otras cosas, el hecho de que la autoridad de protección de datos (APD) ofrezca asesoramiento y orientación a las personas que se dirigen a ella en lugar de limitarse a reenviar las solicitudes; el hecho de que se faciliten modelos de carta para el ejercicio de los derechos de los interesados relativos al Sistema de Información de Schengen II (SIS II) y al Sistema de Información de Visados (VIS); el hecho de que las medidas de seguridad aplicadas en los locales del Departamento de Tecnologías de la Información y Comunicaciones del Ministerio del Interior, que alberga el N.VIS y el N.SIS, sean, en general, de alto nivel, y proporcionen un entorno seguro para el almacenamiento de datos y la prevención de posibles incidentes; la oferta de una formación bien desarrollada a los usuarios finales del VIS, en particular al personal consular antes de su desplazamiento a embajadas o consulados; la determinación de dar formación y desarrollo al personal, y en concreto la existencia una formación bien desarrollada, incluida la relativa a la protección de datos para los usuarios finales del N.SIS y el personal de la Oficina SIRENE; el hecho de que la información facilitada por la APD en su sitio web con respecto al SIS II y al VIS sea muy completa, útil y de fácil acceso (además de estar disponible en varias lenguas); el hecho de que los folletos de la APD sobre la protección de los datos personales en el Sistema de Información de Schengen y sobre la protección de los datos personales en el Sistema de Información de Visados proporcionen información muy buena y accesible sobre el tratamiento de los datos en ambas bases de datos y los correspondientes derechos de los interesados, así como la fuerte implicación de la APD en numerosas conferencias, cursos de formación y otros actos de sensibilización, incluidos los dirigidos al personal que se ocupa del tratamiento de datos del SIS II y del VIS.

(3) En vista de la importancia que reviste el cumplimiento del acervo de Schengen en materia de protección de datos, especialmente con vistas a garantizar la completa independencia de la APD, debe darse prioridad a la aplicación de la recomendación 1.

(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, Lituania 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 Lituania:

en relación con la autoridad de supervisión de la protección de datos

1. a fin de garantizar mejor la total independencia de la Inspección Estatal de Protección de Datos (en lo sucesivo, APD), suprima el requisito de que el plan de acción estratégico de la APD tenga que ser aprobado por el Ministro de Justicia y la obligación de consultar al ministro de Justicia sobre el plan de acción anual antes de que el director de la APD pueda aprobarlo; esto también es importante para garantizar que el procedimiento presupuestario no incluya ningún elemento de riesgo de violación de la independencia de la APD;

2. a fin de garantizar mejor la total independencia de la APD, organice las reuniones bilaterales periódicas entre el ministro de Justicia y el director de la APD de tal manera que no conlleven ningún riesgo de influencia directa o indirecta del Gobierno en la APD, lo que podría poner en peligro la independencia de esta;

3. suprima, de entre los elementos de los cuales el director de la APD debe rendir cuentas al Gobierno y al ministro de Justicia, todos aquellos que puedan conllevar un riesgo de influencia directa o indirecta por parte del Gobierno y del ministro de Justicia y poner en peligro la independencia de la APD;

4. garantice que la APD controle con mayor frecuencia la legalidad del tratamiento de los datos personales del SIS II;

5. garantice que, al menos cada cuatro años, la APD realice auditorías de operaciones de tratamiento de datos en el N.SIS;

6. garantice que la APD controle la legalidad del tratamiento de los datos personales del VIS; durante sus inspecciones de las embajadas, la APD también debería inspeccionar las operaciones de tratamiento de datos y la seguridad de los datos en los proveedores de servicios externos (PSE); esta posibilidad debe especificarse en el contrato entre el Ministerio de Asuntos Exteriores y el PSE;

7. garantice que, al menos cada cuatro años, la APD realice auditorías de las operaciones de tratamiento de datos en el N.VIS;

en relación con los derechos de los interesados

8. garantice que se respete el plazo de respuesta de sesenta días (fijado en el artículo 41, apartado 6, del Reglamento SIS II y en el artículo 58, apartado 6, de la Decisión SIS II) aplicable a las solicitudes de las personas cuyos datos estén en el SIS II, hasta que sea plenamente aplicable (el 28 de diciembre de 2021 a más tardar) el nuevo acervo SIS[2], que remite al plazo de respuesta a las solicitudes de los interesados fijado en el Reglamento General de Protección de Datos (RGPD)[3] (treinta días, con posibilidad de prórroga de dos meses en caso necesario).

9. clarifique los procedimientos internos relativos a la responsabilidad de las autoridades que intervienen en la gestión de los derechos de los interesados en el SIS II; de este modo, el personal también podría tener conocimiento de a quién debe remitir las solicitudes;

---

[2] 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 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).

[3] 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)].

10. garantice que el Ministerio del Interior sea coherente en todas las respuestas finales a las personas que deseen ejercer sus derechos como titulares de datos en el SIS II, de modo que se les facilite información sobre su derecho a recurrir ante la APD y sobre el derecho a interponer un recurso judicial ante los tribunales;

11. clarifique los procedimientos internos relativos a la responsabilidad de las autoridades que intervienen en la gestión de los derechos de los interesados en el VIS; de este modo, el personal también podría tener conocimiento de a quién debe remitir las solicitudes;

12. garantice que el Ministerio del Interior sea coherente en todas las respuestas finales a las personas que deseen ejercer sus derechos como titulares de datos en el VIS, de modo que se les facilite información sobre su derecho a recurrir ante la APD y sobre el derecho a interponer un recurso judicial ante los tribunales;

en relación con el Sistema de Información de Visados

13. adopte las medidas necesarias para garantizar que los contratos entre el Ministerio Asuntos Exteriores y los PSE regulen la forma en que la APD de Lituania puede participar en las inspecciones llevadas a cabo por las embajadas y consulados y por el propio Ministerio;

14. mejore el autocontrol verificando de forma proactiva y regular los registros con el fin de controlar la legalidad del tratamiento de los datos personales del VIS; el Ministerio del Interior debería seguir desarrollando el sistema SIEM para el control automático de los registros;

15. garantice que el responsable de protección de datos del Ministerio Asuntos Exteriores esté más involucrado en el desarrollo y la oferta de formación en materia de protección de datos dirigida a los miembros del personal del Ministerio, incluidos los destinados en embajadas o consulados;

en relación con el Sistema de Información de Schengen II

16. elimine la posibilidad de que un usuario final se registre a través del navegador POLIS en el N.SIS con varios dispositivos al mismo tiempo;

17. garantice la introducción de tarjetas inteligentes para el acceso a los puestos de trabajo de los usuarios del N.SIS en la policía, con el fin de mejorar el nivel de seguridad;

18. se asegure de que las medidas técnicas adoptadas para evitar el uso de llaves USB en los puestos de trabajo de las oficinas SIRENE se apliquen y se controlen de manera periódica;

19. mejore el autocontrol verificando de forma proactiva y regular los registros de los usuarios finales del SIS II pertenecientes a todas las autoridades afectadas con el fin de controlar la legalidad del tratamiento de los datos personales del SIS II; el Ministerio del Interior debería seguir desarrollando el sistema SIEM para el control automático de los registros;

20. se asegure de que el personal tome mayor conciencia de la importancia de la protección de datos en relación con la manipulación de los datos del SIS II y del VIS, ofreciéndole regularmente sesiones de reciclaje;

21. se asegure de que el grupo de responsables de protección de datos del Ministerio del Interior dirija la formación y la sensibilización del personal que tenga acceso al N.SIS; se podría garantizar así la continuidad en la estructura y la planificación de la formación del personal;

en relación con la información pública

22. garantice la actualización periódica de los enlaces de la página web de la APD relativos al SIS II y al VIS;

23. garantice que los sitios web de los departamentos que mantienen contactos con nacionales de otros países —como el Ministerio del Interior, la Policía, el Servicio de la Guardia de Fronteras del Estado, el Ministerio Asuntos Exteriores y las oficinas consulares— ofrezcan información accesible y clara sobre el SIS II y el VIS y sobre los correspondientes derechos de los interesados, también en inglés;

24. garantice que, cuando los sitios web proporcionen información sobre el SIS II y el VIS y los correspondientes derechos de los interesados en inglés, esta información sea más fácil de encontrar;

25. garantice la coherencia de la información sobre el ejercicio de los derechos de los interesados en relación con el N.SIS II y el VIS facilitada en los sitios web de las instituciones que trabajen con dichos sistemas;

26. añada información sobre el tratamiento de datos y los derechos de los interesados en relación con el VIS al portal EPM a través del cual las personas facilitan información sobre las solicitudes de visado.

Hecho en Bruselas, el

Por el Consejo
El Presidente / La Presidenta