Conselho da
União Europeia

Bruxelas, 25 de janeiro de 2021
(OR. en)

5534/21

Dossiê interinstitucional:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
para:	Delegações
n.º doc. ant.:	14250/20
Assunto:	Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2019 relativa à aplicação, pela **Eslováquia**, do acervo de Schengen no domínio da **proteção de dados**

Junto se envia, à atenção das delegações, a Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2019 relativa à aplicação, pela Eslováquia, do acervo de Schengen no domínio da proteção de dados, adotada por procedimento escrito em 21 de janeiro de 2021.

Nos termos do artigo 15.º, n.º 3, do Regulamento (UE) n.º 1053/2013 do Conselho, de 7 de outubro de 2013, a presente recomendação será transmitida ao Parlamento Europeu e aos parlamentos nacionais.

Decisão de Execução do Conselho que estabelece uma

RECOMENDAÇÃO

para suprir as deficiências identificadas na avaliação de 2019 relativa à aplicação, pela Eslováquia, do acervo de Schengen no domínio da proteção de dados

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) n.º 1053/2013 do Conselho, de 7 de outubro de 2013, que cria um mecanismo de avaliação e de monitorização para verificar a aplicação do acervo de Schengen e que revoga a Decisão do Comité Executivo de 16 de setembro de 1998, relativa à criação de uma comissão permanente de avaliação e de aplicação de Schengen[1], nomeadamente o artigo 15.º,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

(1) O objetivo da presente decisão é recomendar à República Eslovaca que tome medidas corretivas para suprir as deficiências identificadas durante a avaliação de Schengen de 2019 no domínio da proteção de dados. Na sequência dessa avaliação, foi adotado, pela Decisão de Execução C(2020) 8160 da Comissão, um relatório que contém conclusões e apreciações, bem como uma lista das melhores práticas e das deficiências identificadas durante a avaliação.

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

(2) Consideram-se boas práticas, nomeadamente o facto de, desde a última avaliação de Schengen em 2012, a autoridade de proteção de dados (APD) realizar regularmente atividades de supervisão do SIS II, de acordo com um planeamento anual, e de ter sido elaborado um conjunto de princípios aplicável às inspeções do SIS II nos próximos quatro anos; o facto de a APD ter realizado um número considerável de inspeções aos consulados; os esforços realizados pela APD e pelo Ministério do Interior (MI) para fornecer informações aos titulares dos dados em suporte eletrónico e em papel; o facto de existirem versões em várias línguas das informações sobre temas relacionados com Schengen no sítio Web da APD e nos folhetos; o facto de a APD fornecer modelos para os pedidos dos titulares dos dados do SIS e do VIS; o facto de o gabinete SIRENE responder aos pedidos não apenas em língua eslovaca, mas também em inglês; o facto de as autoridades eslovacas informarem os titulares dos dados se não estiverem armazenados no SIS II nenhuns dado a seu respeito; o sistema de controlo muito ativo do VIS e do SIS II pela Secção de Inspeção do Serviço de Inspeção do MI; o papel muito ativo dos dois membros do pessoal no Departamento de Segurança do Ministério dos Negócios Estrangeiros e dos Assuntos Europeus (MNEAE) encarregados dos assuntos relativos à proteção de dados; que o MNEAE dê formação em matéria de proteção de dados ao seu pessoal, em especial antes do destacamento temporário para funções consulares, e que o Departamento de Segurança (na sua função de gabinete de proteção de dados) dê essa formação; o facto de a segurança processual e física criada para proteger os dados do SIS II ser de alto nível; o papel muito ativo que o responsável pela proteção de dados e o seu adjunto no Departamento de Proteção de Dados da Unidade de Inspeção do Serviço de Inspeção do MI exercem, inclusive no que toca às orientações e ao controlo dos registos relativos ao SIS II; o facto de o MI dar formação em matéria de proteção de dados a todos os utilizadores finais do N.SIS II.

(3) Atendendo à importância de dar cumprimento ao acervo de Schengen em matéria de proteção de dados relativamente ao VIS, deverá ser dada prioridade à execução das recomendações 7 e 24.

(4) A presente decisão deverá ser enviada ao Parlamento Europeu e aos parlamentos dos Estados-Membros. No prazo de três meses a contar da sua adoção, a República Eslovaca deverá, por força do artigo 16.º, n.º 1, do Regulamento (UE) n.º 1053/2013, apresentar um plano de ação que contenha todas as recomendações, destinado a corrigir as deficiências identificadas no relatório de avaliação, o qual deverá enviar à Comissão e ao Conselho,

RECOMENDA

que a República Eslovaca:

Autoridade de Proteção de Dados

1. A fim de reforçar o desempenho e a eficácia da APD, assegure que o orçamento e os efetivos da APD continuem a aumentar;

2. Assegure que a parte do orçamento geral prevista para a APD seja claramente visível, a fim de garantir que a APD disponha de um orçamento anual público separado;

3. Assegure que, no processo orçamental, o Conselho Nacional seja informado da posição da APD quanto às suas necessidades orçamentais e nos debates em matéria orçamental entre a APD e o Ministério das Finanças (MF);

4. Tome medidas para que o MF não possa estabelecer qualquer correlação entre o orçamento e o montante das coimas a cobrar pela APD, uma vez que tal poderia ter repercussões sobre a natureza e a definição de prioridades do trabalho da APD e assim afetar a sua independência. Deverá garantir-se que o orçamento da APD não possa ser reduzido durante o ano civil numa situação em que as multas estimadas não tenham sido integralmente cobradas pela APD;

5. Assegure que sejam atribuídas à APD todas as funções e poderes previstos para as autoridades de proteção de dados nos artigos 57.º e 58.º do RGPD;

6. Assegure que, para além das atividades de supervisão regularmente realizadas no serviço N.SIS e no Gabinete SIRENE, a APD exerça uma maior supervisão sobre as autoridades utilizadoras finais que têm acesso ao SIS II;

7. Assegure que das atividades de supervisão da APD em relação ao VIS faça parte a inspeção da Autoridade Central de Vistos (ACV) no que diz respeito às operações de tratamento de dados no N.VIS. Uma vez que o prazo para a primeira auditoria do sistema nacional de vistos terminou em outubro de 2015, a APD deverá realizar, o mais rapidamente possível, a parte da auditoria que ainda está em falta;

8. Assegure que a APD realize também regularmente inspeções aos prestadores de serviços externos;

Direitos dos titulares dos dados

9. Encontre uma forma adequada de a APD, o MI e o MNEAE informarem os titulares dos dados sobre os riscos potenciais do envio de cópias de documentos de identificação e de informações sensíveis através da Internet aberta. O MI e o MNEAE deverão ponderar a possibilidade de proporcionar aos titulares de dados uma via de transmissão eletrónica segura para este tipo de documentos;

10. Assegure que o prazo de 60 dias para responder aos pedidos dos titulares de dados do SIS II previsto no artigo 41.º, n.º 6, do Regulamento SIS II e no artigo 58.º, n.º 6, da Decisão SIS II seja respeitado, até que o novo acervo do SIS[1] seja plenamente aplicável (o mais tardar até 28 de dezembro de 2021), no qual é feita referência ao prazo de resposta aos pedidos dos titulares dos dados previsto no RGPD (30 dias com a possibilidade de prorrogação por mais dois meses, se necessário);

11. Estude a possibilidade de fornecer algumas das informações impressas (folhetos/sinais, etc.) aos titulares de dados nas esquadras de polícia, assegurando a sua visibilidade e facilidade de acesso;

12. Pondere a possibilidade de apresentar, por exemplo, uma versão inglesa informal das decisões da APD sobre as queixas relativas aos pedidos dos titulares dos dados do SIS II, o que ajudaria os titulares dos dados a compreender melhor a decisão e reforçaria os seus direitos;

13. Assegure que, no sítio Web do MNEAE, as informações sobre os direitos dos titulares dos dados do VIS sejam mais fáceis de encontrar; este sítio deverá igualmente fornecer modelos para os pedidos dos titulares dos dados do VIS;

---

[1] Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão, JO L 312 de 7.12.2018, p. 56 (ver, em especial, os artigos 66.º a 71.º). Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006, JO L 312 de 7.12.2018, p. 14 (ver, em especial, os artigos 51.º a 57.º).

14. Assegure que o formulário de pedido de visto contenha informações claras sobre as diferentes autoridades que tratam os dados pessoais no âmbito do sistema nacional de vistos. Importa, em especial, informar que o responsável pelo tratamento dos dados é o MNEAE;

15. Forneça informações impressas (folhetos/sinais, etc.) aos titulares de dados do VIS nos aeroportos e postos de controlo fronteiriço, assegurando a sua visibilidade e facilidade de acesso;

16. Assegure que as respostas enviadas aos titulares de dados pessoais do VIS forneçam informações sobre a possibilidade de recorrer da resposta junto da APD e do tribunal competente;

17. Tome as medidas necessárias para clarificar as responsabilidades que cabem ao MNEAE e à ACV quanto ao tratamento dos pedidos dos titulares dos dados do VIS e à emissão de orientações internas ou metodológicas para ambas as entidades; estas informações deverão estar ao dispor dos titulares dos dados;

Sistema de Informação sobre Vistos

18. Tome as medidas necessárias para aumentar o nível de segurança do acesso ao ambiente da administração do Estado e, em especial, aos pedidos de visto nacionais no MNEAE e no MI (Autoridade central responsável pelos vistos), nomeadamente através do acesso às bases de dados nacionais de vistos com tecnologia multifatores;

19. Tome as medidas necessárias para aumentar a segurança física e organizativa no centro de dados N.VIS do MNEAE, em particular no que respeita aos seguintes aspetos:

    – Criação de um livro de registo de visitantes à entrada do centro de dados para o pessoal informático, os visitantes ou os fornecedores cujo acesso deva ser limitado;

    – Instalação de um sistema de extinção de incêndios com gás (aragonite);

    – Instalação de deteção de fugas de água,

    – Arrumação e limpeza dos pavimentos;

    – Fecho da vedação de proteção dos servidores da UE;

20. Acelere o processo de criação de um novo centro de dados N.VIS noutro local e a reinstalação do centro de dados;

21. Avalie a possibilidade de alterar o período de conservação local dos ficheiros de registo N.VIS nas missões diplomáticas e consulares, fixando um prazo em vez da quantidade de MB;

22. Pondere a utilização de sistemas de controlo automático dos registos no MNEAE;

23. Tome as medidas necessárias para que as missões diplomáticas ou o MFAE efetuem regularmente inspeções aos prestadores de serviços externos;

24. Tome as medidas necessárias para assegurar uma formação mais sistemática e uniforme do pessoal consular local em matéria de proteção de dados;

25. Assegure que sejam exigidas as mesmas informações para o pedido de visto eletrónico que para o formulário de pedido de visto em papel (tal como previsto no anexo I do Código de Vistos da UE[1]);

Sistema de Informação de Schengen II

26. Tome as medidas necessárias para aumentar o nível de segurança do acesso ao N.SIS II, nomeadamente por meio da autenticação multifatores e do acesso ao N.SIS II exclusivamente por ligações "https";

27. Assegure que o MI informe a APD de qualquer violação de dados suscetível de implicar riscos para os direitos e liberdades das pessoas singulares. Além disso, o MI deverá criar um registo das violações de dados pessoais;

---

[1] Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (Código de Vistos). JO L 243 de 15.9.2009, p. 1.

Sensibilização do público

28. Estude a possibilidade de colocar folhetos da APD à disposição dos titulares de dados em locais mais acessíveis, como as esquadras de polícia, os postos de controlo fronteiriço e as instalações consulares;

29. Avalie a possibilidade de realizar exposições, seminários e eventos de portas abertas também acessíveis ao grande público, em especial aos titulares dos dados, uma vez que estes têm interesse nas informações sobre o SIS II e o VIS;

Feito em Bruxelas, em

Pelo Conselho
O Presidente