Conselho da
União Europeia

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

5533/21

Dossiê interinstitucional:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
para:	Delegações
n.º doc. ant.:	14247/20
Assunto:	Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2019 relativa à aplicação, pela **Hungria**, 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 Hungria 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 Hungria, 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) A presente decisão tem por objetivo recomendar à Hungria que tome medidas corretivas para suprir as deficiências identificadas durante a avaliação Schengen de 2019 no domínio da proteção de dados. Na sequência dessa avaliação, foi adotado, pela Decisão de Execução C(2020) 8170 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 o orçamento da autoridade nacional para a proteção dos dados e a liberdade de informação (NAIH) ter registado um aumento constante, de o Gabinete SIRENE ter cumprido as recomendações formuladas em 2012 na anterior avaliação de Schengen em matéria de proteção de dados, e de existir agora a possibilidade de os titulares dos dados apresentarem queixa à NAIH; de o Ministério dos Negócios Estrangeiros e do Comércio (MNEC) se referirem também à possibilidade de recurso judicial; de as informações fornecidas no sítio Web da NAIH serem completas e úteis, estarem disponíveis e claramente formuladas e poderem ser facilmente consultadas; de o MNEC ter envidado esforços para gerir e formalizar os diferentes aspetos da segurança da informação; de o MNEC dispor de um plano de segurança robusto e completo e de os modelos para o exercício dos direitos dos titulares dos dados do Sistema de Informação Schengen (SIS) II se encontrarem disponíveis em várias línguas (húngaro, inglês, alemão, francês e russo).

(3) Não deverá ser dada nenhuma indicação de prioridade para o cumprimento das recomendações.

(4) A presente decisão deverá ser enviada ao Parlamento Europeu e aos parlamentos dos Estados-Membros. No prazo de seis meses a contar da sua adoção, a Hungria deverá, por força do artigo 16.º, n.º 8, do Regulamento (UE) n.º 1053/2013, apresentar à Comissão uma avaliação das (eventuais) correções e uma descrição das medidas necessárias,

RECOMENDA

que a Hungria:

Autoridade de proteção de dados (NAIH)

1. Assegure que a NAIH, ao exercer a supervisão do cumprimento da legislação do SIS II, proceda a inspeções regulares das indicações do SIS II;

2. Assegure que a NAIH dê seguimento às conclusões e recomendações das inspeções e auditorias do SIS II resultantes de medidas de supervisão anteriores e que as mesmas sejam também tidas em conta nos planos de inspeção de 2019;

3. Assegure que a NAIH realize um acompanhamento global da aplicação efetiva das recomendações do Sistema de Informação sobre Vistos (VIS) em matéria de atividades de supervisão;

4. Assegure que a atividade de supervisão da NAIH abranja todos os aspetos da proteção de dados do sistema nacional de vistos, incluindo o tratamento por parte de prestadores de serviços externos;

Direitos dos titulares dos dados

5. Alargue o âmbito de aplicação do anexo 9 do decreto governamental n.º 15/2013 (que estabelece um modelo específico para o exercício dos direitos de acesso dos titulares dos dados), a fim de estabelecer também modelos para o exercício dos outros direitos dos titulares, como a correção e a supressão dos dados;

6. Assegure que as autoridades húngaras (Direção-Geral Nacional da Polícia de Estrangeiros — DGNPE) clarifiquem os procedimentos que seguem para a avaliação dos pedidos dos titulares dos dados, em especial quando limitem os direitos de retificação ou supressão, e os alinhem pelo direito aplicável da União e nacional;

Sistema de informação sobre vistos

7. Assegure que os utilizadores privilegiados do VIS sejam suficientemente monitorizados; nesta perspetiva, podem ser necessárias medidas organizativas e técnicas para monitorizar os utilizadores privilegiados;

8. Aumente a frequência dos testes de gestão da continuidade das atividades e do plano de recuperação em caso de catástrofe, em especial no caso do MNEC;

9. Assegure que, até ao lançamento do sítio informático secundário, não sejam armazenadas todas as cópias de segurança nas mesmas instalações que o servidor, mas que o sejam noutro local;

10. Aumente a segurança do acesso ao espaço de armazenamento;

11. Proceda regularmente a uma verificação da segurança do sistema de encriptação desenvolvido a nível interno (MNEC);

Sistema de Informação de Schengen

12. Aumente a segurança física do edifício do centro de dados dotando também a segunda saída/entrada de videovigilância e reforce a segurança física do espaço de armazenamento na sala do servidor;

13. Proceda regularmente a verificações da segurança do sistema de gestão do acesso dos utilizadores do SIS II;

14. Assegure a utilização de diretrizes/orientações gerais uniformes em matéria de segurança das informações do N.SIS (por exemplo, as regras aplicáveis às senhas, etc.);

15. Assegure que o gabinete SIRENE explore, em cooperação com o Arquivo Nacional, as possibilidades de aumentar a frequência do procedimento de seleção no que toca à conservação de dados;

16. Aumente a frequência dos testes da gestão da continuidade das atividades e do plano de recuperação em caso de catástrofe;

17. Assegure que o Quartel-General da Polícia Nacional da Hungria (OFRK), em particular o Serviço N.SIS e o Gabinete SIRENE, instalem uma solução para monitorizar os utilizadores privilegiados;

18. Assegure que o gabinete SIRENE exerça uma função mais ativa no que toca à coordenação das atividades de verificação da qualidade das informações inseridas no SIS II, como se descreve no artigo 1.15 do Manual SIRENE;

Sensibilização do público

19. Assegure que o MNEC defina claramente quem é o responsável ou responsáveis pelo tratamento de dados do VIS. Para garantir a transparência e permitir que os cidadãos exerçam os seus direitos, é importante que os titulares dos dados sejam devidamente informados das competências de cada responsável pelo tratamento de dados;

20. Assegure que o ORFK atualize regularmente a versão inglesa que contém a secção relativa ao SIS;

Feito em Bruxelas, em

Pelo Conselho
O Presidente