Conselho da
União Europeia

Bruxelas, 24 de setembro de 2019
(OR. en)

12469/19

Dossiê interinstitucional:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	20 de setembro de 2019
para:	Delegações
n.º doc. ant.:	11906/1/19 REV 1
Assunto:	Decisão de execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2018 relativa à aplicação pela **Letónia** 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 2018 da aplicação pela Letónia do acervo de Schengen no domínio da proteção de dados, adotada pelo Conselho na sua reunião realizada a 20 de setembro de 2019.

Em conformidade com o 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 enviada ao Parlamento Europeu e aos parlamentos nacionais.

Decisão de execução do Conselho que estabelece uma

RECOMENDAÇÃO

para suprir as deficiências identificadas na avaliação de 2018 relativa à aplicação pela Letónia 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 Letónia medidas corretivas para suprir as deficiências identificadas durante a avaliação de Schengen de 2018 no domínio da proteção de dados. Na sequência dessa avaliação, foi adotado, pela Decisão de Execução C(2019)5720 da Comissão, um relatório com conclusões e apreciações, bem como uma lista das boas práticas e das deficiências detetadas durante a avaliação.

(2) Como boas práticas observou-se, nomeadamente, a aplicação com êxito do financiamento da Comissão Europeia para melhorar a sensibilização do público e o facto de as respostas do Gabinete SIRENE estarem disponíveis em várias línguas e serem geralmente comunicadas num curto espaço de tempo.

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

(3) Tendo em conta a importância do cumprimento do acervo de Schengen em matéria de proteção de dados no âmbito do Sistema de Informação Schengen II (SIS II), deverá ser dada prioridade às recomendações 15 a 18.

(4) Tendo em conta a importância do cumprimento do acervo de Schengen em matéria de proteção de dados no âmbito do Sistema de Informação sobre Vistos (VIS), deverá ser dada prioridade às recomendações 9 a 11.

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

RECOMENDA:

A Letónia deverá:

Autoridade de controlo da proteção de dados

1. Assegurar a total independência da Autoridade de Proteção de Dados (APD) através da adoção de legislação nacional que cumpra o disposto no capítulo VI do Regulamento Geral sobre a Proteção de Dados (RGPD), em especial o procedimento de demissão do diretor;

2. Assegurar que a Autoridade de Proteção de Dados recebe financiamento suficiente e mantém um nível adequado de efetivos a fim de poder cumprir todas as tarefas que lhe são confiadas no âmbito do acervo do Sistema de Informação de Schengen II (a seguir designado "SIS II") e do Sistema de Informação sobre Vistos (a seguir designado "VIS");

3. Assegurar a realização em tempo útil da auditoria das operações de tratamento de dados no N.SIS, como previsto no artigo 44.º, n.º 2, do Regulamento SIS II, e no artigo 60.º, n.º 2, da Decisão SIS II do Conselho;

4. Assegurar a realização em tempo útil da auditoria das operações de tratamento de dados no NVIS, como previsto no artigo 41.º, n.º 2, do Regulamento VIS, e no artigo 8.º, n.º 6, da Decisão VIS do Conselho;

5. Assegurar que as futuras auditorias relativas ao SIS II e ao VIS são exaustivas e efetuadas de acordo com as normas internacionais de auditoria, como exigido pelo acervo destes dois sistemas, e com recurso às necessárias competências em tecnologias da informação;

6. Assegurar que as atividades de supervisão da APD em relação ao SIS II incluem controlos regulares das indicações do SIS II;

7. Assegurar que as atividades de supervisão da APD em relação ao VIS incluem controlos regulares dos postos consulares;

8. Assegurar que o plano de inspeção plurianual da APD inclui outras atividades de inspeção diferentes das auditorias obrigatórias do SIS II e do VIS;

Sistema de Informação sobre Vistos

9. Assegurar que os registos são regularmente analisados para efeitos de controlo da legalidade das atividades de tratamento de dados, em conformidade com o artigo 34.º, n.ºs 1 e 2, do Regulamento VIS;

10. Clarificar qual o papel exato (encarregado do tratamento de dados ou responsável conjunto) do Ministério dos Negócios Estrangeiros (a seguir designado "MNE") em relação ao Gabinete dos Assuntos de Cidadania e Migração (a seguir designado "GACM");

11. Assegurar auditorias internas mais frequentes às atividades de tratamento no VIS pelo GACM;

12. Rever os contratos com prestadores de serviços externos a fim de garantir o seu respeito e alinhamento com os requisitos estabelecidos no RGPD;

13. Definir claramente as atribuições e competências dos responsáveis pela proteção de dados no âmbito do GACM e do MNE, respetivamente;

14. Assegurar que os formulários em linha utilizados no contexto de um pedido de visto incluem uma advertência sobre a proteção de dados informando os titulares de dados das atividades de tratamento de dados e dos direitos individuais aplicáveis;

Sistema de Informação de Schengen

15. Assegurar que a polícia realiza regularmente auditorias internas, em especial o controlo interno dos registos;

16. Gerar registos nacionais do SIS II a nível central e assegurar que a justificação para a consulta possa ser determinada a partir do registo;

17. Assegurar que os ficheiros dos registos são revistos regularmente, a fim de verificar a licitude do tratamento de dados em conformidade com o artigo 12.º, n.º 2, do Regulamento SIS II e da Decisão SIS II do Conselho;

18. Minimizar o risco para a segurança decorrente da aplicação móvel que permite o acesso ao SIS II unicamente através, por exemplo, da disponibilização de acesso a partir de um serviço VPN;

19. Criar um sistema de autenticação de dois fatores;

20. Assegurar que a produção de dados não é utilizada para fins de teste e que apenas os utilizadores autorizados podem proceder a pesquisas no NSIS;

21. Definir claramente as atribuições e competências do responsável pela proteção de dados a nível da polícia, incluindo a sua participação nas atividades de controlo interno, nomeadamente no que respeita à eficácia das medidas de segurança;

Direitos dos titulares de dados e sensibilização

22. Comunicar regularmente à APD as estatísticas relativas ao exercício dos direitos dos titulares de dados no respeitante ao SIS II e ao VIS;

23. Disponibilizar mais material informativo, como a brochura "Dados pessoais no Sistema de Informação de Schengen", no aeroporto e noutros locais públicos.

Feito em Bruxelas, em

Pelo Conselho
O Presidente