Conselho da
União Europeia

Bruxelas, 8 de março de 2019
(OR. en)

7281/19

Dossiê interinstitucional:
2019/0024(NLE)

SCH-EVAL 50
DATAPROTECT 84
COMIX 148

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	7 de março de 2019
para:	Delegações
n.º doc. ant.:	6399/19
Assunto:	Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2018 relativa à aplicação pela **Suíça** 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 Suíça do acervo de Schengen no domínio da proteção de dados, adotada pelo Conselho na sua reunião realizada a 7 de março 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.

ANEXO

Decisão de Execução do Conselho que estabelece uma

RECOMENDAÇÃO

para suprir as deficiências identificadas na avaliação de 2018 relativa à aplicação pela Suíça 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 Suíça 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, mediante a Decisão de Execução C(2019) 200 da Comissão, um relatório que inclui 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) São consideradas boas práticas, nomeadamente, o guia sobre "Controlo da utilização do Sistema de Informação de Schengen (SIS)" elaborado pelo Grupo de Coordenação de Schengen estabelecido pelas autoridades suíças de proteção de dados; que o sítio Web do gabinete do Comissário Federal para a Proteção de Dados e Informação (FDPIC) contém um conjunto abrangente de formulários específicos para o exercício dos direitos dos titulares de dados relacionados com o Sistema de Informação de Schengen (SIS II), o Sistema de Informação sobre Vistos (VIS), bem como muito boa informação nas suas perguntas frequentes relacionadas com o SIS II, "Schengen… e os seus dados pessoais", e com o VIS, "O VIS Schengen e os seus dados pessoais"; a rapidez das respostas do Serviço Federal de Polícia (Fedpol) aos pedidos dos titulares de dados, tendo em conta, nomeadamente, o número significativo de pedidos recebidos; o facto de as medidas de segurança aplicadas nas instalações do centro de serviços informáticos do ISC-FDJP (onde estão situados os servidores do N-VIS e SIS II) serem de alto nível, proporcionando um ambiente seguro para armazenar dados e para evitar eventuais incidentes; os esforços significativos da Fedpol no que respeita à formação e sensibilização do seu pessoal, nomeadamente para as questões de proteção de dados; a participação ativa dos responsáveis pela proteção de dados (RPD) da Fedpol, em especial na formação e aconselhamento sobre todas as questões relativas à proteção de dados e no tratamento dos pedidos dos titulares dos dados.

(3) Atendendo à importância de dar cumprimento ao acervo de Schengen no domínio da proteção dos dados do SIS II e do VIS, deverá ser dada prioridade à execução das recomendações 12 e 15.

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

RECOMENDA:

a Suíça deverá

Autoridades de proteção de dados

1. A fim de assegurar melhor a plena independência do Comissário Federal para a Proteção de Dados e Informação (FDPIC), ponderar a abolição, no quadro da revisão da Lei Federal de proteção de dados, da possibilidade de o FDPIC exercer uma atividade secundária;

2. A fim de assegurar melhor a plena independência da APD do cantão de Lucerna, abolir a possibilidade de exonerar o Comissário para a Proteção de Dados de Lucerna por "motivos justificados" (que não seja uma falta grave);

3. Reforçar os poderes executivos do FDPIC, de modo a permitir-lhe tomar diretamente decisões juridicamente vinculativas;

4. Reforçar os poderes executivos das autoridades cantonais responsáveis pela proteção de dados, atribuindo-lhes o direito de tomar diretamente decisões juridicamente vinculativas;

5. Afetar recursos financeiros e humanos suficientes ao FDPIC para que possa cumprir as funções que lhe são confiadas no âmbito do acervo do SIS II e do VIS.

6. Afetar recursos financeiros e humanos suficientes à APD do cantão de Lucerna para que possa cumprir as funções que lhe são confiadas no âmbito do acervo do SIS II e do VIS.

7. A fim de melhor garantir a plena independência da APD do cantão de Lucerna, permitir que esta nomeie o seu próprio pessoal de acordo com as suas necessidades;

8. A fim de assegurar melhor a total independência do FDPIC, reformar o procedimento orçamental, de forma que exerça uma influência real sobre a proposta do respetivo orçamento antes de a proposta de orçamento geral ser enviada ao Parlamento para debate e adoção, bem como que a proposta orçamental do FDPIC seja comunicada ao Parlamento;

9. A fim de assegurar a total independência da APD do cantão de Lucerna, reformar o procedimento orçamental, de forma que a APD do cantão de Lucerna exerça uma influência real sobre a proposta do respetivo orçamento antes de a proposta de orçamento geral ser enviada ao Parlamento para debate e adoção; a APD do cantão de Lucerna deverá dispor de autonomia orçamental, por forma a poder influenciar e controlar as decisões orçamentais que lhe digam respeito;

10. Assegurar que o FDPIC controla com maior frequência a legalidade do tratamento dos dados pessoais do SIS II; Estas inspeções deverão continuar a incluir o controlo dos ficheiros de registos, mas deverão abranger também os outros aspetos da proteção de dados relacionados com a estrutura e o funcionamento do N-SIS II;

11. Assegurar que a APD do cantão de Lucerna controla com maior frequência a legalidade do tratamento dos dados pessoais do SIS II;

12. Assegurar que as auditorias das operações de tratamento de dados no N.SIS são efetuadas pelo FDPIC pelo menos de quatro em quatro anos; esta auditoria deverá abranger também as operações de tratamento de dados no N-SIS II pelo responsável pelo tratamento dos dados do N-SIS II, nomeadamente da Fedpol, incluindo o SIRENE B e o servidor N-SIS; Dado que o prazo para a primeira auditoria era abril de 2017, deverão ser tomadas medidas para cumprir esta obrigação o mais rapidamente possível;

13. Assegurar que o FDPIC controla com maior frequência a legalidade do tratamento dos dados pessoais do VIS;

14. Assegurar que a APD do cantão de Lucerna controla com maior frequência a legalidade do tratamento dos dados do Sistema de Informação sobre Vistos (VIS);

15. Assegurar que as auditorias das operações de tratamento de dados no sistema VIS nacional (ORBIS) são efetuadas pelo FDPIC pelo menos de quatro em quatro anos; Dado que o prazo para a primeira auditoria (outubro de 2015) não foi respeitado, deverão ser tomadas medidas para que a auditoria em curso seja concluída o mais rapidamente possível.

Direitos dos titulares dos dados

16. Ponderar cuidadosamente a forma como os direitos relacionados com o SIS II dos titulares de dados residentes no estrangeiro podem ser assegurados de forma mais eficaz, dado que a legislação suíça exige que as decisões formais (casos de recusa de acesso aos dados pessoais) devem ser enviadas para um endereço suíço;

17. Disponibilizar informações nos sítios Web da Fedpol e do FDPIC e sobre a possibilidade de os titulares de dados recorrerem para os tribunais nos casos em que o prazo para dar resposta aos pedidos relacionados com o SIS II de titulares dos dados (60 dias) não é respeitado;

18. Assegurar que todos os sítios Web das autoridades policiais dos cantões facultem informações básicas sobre a proteção de dados e ligações diretas aos sítios Web das APD dos cantões;

19. Assegurar que as diferentes autoridades de controlo da proteção de dados, a nível federal e cantonal, dispõem de recursos adequados para cumprir plenamente a sua obrigação de defender e apoiar o exercício dos direitos dos titulares dos dados, incluindo o tratamento das queixas que lhes são apresentadas pelos cidadãos;

20. Fornecer informações sobre a base jurídica para o exercício dos direitos dos titulares dos dados (incluindo informações sobre o que se consideram pedidos repetitivos/abusivos) na secção "perguntas mais frequentes" (FAQ) e nos sítios Web da Fedpol, do FDPIC, do cantão de Lucerna e nas embaixadas e consulados no estrangeiro;

Sistema de Informação sobre Vistos

21. Acrescentar elementos sobre a proteção de dados à formação intensiva de dois meses ministrada pela Secretaria de Estado das Migrações (SEM) ao pessoal responsável pelos vistos;

22. Assegurar que a SEM realiza proativamente verificações regulares dos registos, a fim de controlar a legalidade do tratamento dos dados pessoais do VIS;

23. Assegurar que, em geral, a SEM reforça as suas medidas de auditoria interna exigidas nos termos do artigo 32.º, n.º 2, alínea k), do Regulamento VIS e no artigo 9.º, n.º 2, alínea k), da Decisão do Conselho relativa ao VIS;

Sistema de Informação de Schengen

24. Assegurar que a Fedpol põe em prática medidas técnicas para impedir a utilização de portas USB nos terminais com acesso ao N-SIS II;

25. Assegurar que as missões no estrangeiro, aeroportos, esquadras de polícia e serviços de migração dos cantões disponibilizam ao público, nas suas instalações, versões em papel do folheto "Schengen e os seus dados pessoais";

26. Verificar e redefinir se é tecnicamente possível que os utilizadores autorizados do N-SIS II possam ter sessões simultâneas em meios diferentes (por exemplo, através de um terminal fixo e de um dispositivo móvel); atualizar os documentos internos de segurança da informação, a fim de evitar a possibilidade de haver sessões simultâneas no N-SIS II através de meios diferentes;

27. Assegurar que a Fedpol realiza proativamente verificações regulares dos registos, a fim de controlar a legalidade do tratamento dos dados pessoais do SIS II;

28. Assegurar que, em geral, a Fedpol reforça as medidas de auditoria interna exigidas nos termos do artigo 10.º, n.º 1, alínea k), do Regulamento SIS II e no artigo 10.º, n.º 1, alínea k), da Decisão do Conselho relativa ao SIS II;

Sensibilização do público

29. Assegurar que o material de informação sobre os direitos dos titulares dos dados do VIS é mais fácil de encontrar e se encontra sinalizado de forma mais clara no sítio Web do FDPIC, bem como disponibilizando igualmente em inglês os sítios Web da SEM, da polícia cantonal e das APD cantonais;

30. Assegurar que as missões no estrangeiro, aeroportos, esquadras de polícia e serviços de migração dos cantões disponibilizam ao público, nas suas instalações, versões em papel do folheto "Schengen e os seus dados pessoais";

Feito em Bruxelas, em

Pelo Conselho
O Presidente