Conselho da
União Europeia

Bruxelas, 14 de maio de 2018
(OR. en)

8792/18

Dossiê interinstitucional:
2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	14 de maio de 2018
para:	Delegações
n.º doc. ant.:	8285/18
Assunto:	Decisão de execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2017 relativa à aplicação por **Portugal** do acervo de Schengen no domínio da **proteção de dados**

Envia-se em anexo, à atenção das delegações, a Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2017 relativa à aplicação por Portugal do acervo de Schengen no domínio da proteção de dados, adotada pelo Conselho na reunião de 14 de maio de 2018.

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 2017 relativa à aplicação por Portugal 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 a Portugal medidas corretivas para suprir as deficiências identificadas durante a avaliação Schengen de 2017 no domínio da proteção de dados. Na sequência dessa avaliação, foi adotado, através da Decisão de Execução [C(2018)1190] da Comissão, um relatório que inclui conclusões e apreciações, bem como uma lista das boas práticas e deficiências identificadas durante a avaliação.

(2) A equipa no terreno congratulou-se com o investimento contínuo da autoridade de proteção de dados na formação do seu pessoal técnico, que considera um exemplo de boas práticas.

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

(3) Atendendo à importância de respeitar o acervo de Schengen, em particular a obrigação de assegurar e exercer eficazmente a supervisão e de garantir as necessárias medidas de segurança, deverá ser atribuída prioridade à aplicação das recomendações 1, 4, 14, 17 e 22.

(4) 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, Portugal deve, por força do artigo 16.º, n.º 1, do Regulamento (UE) n.º 1053/2013, elaborar um plano de ação destinado a corrigir as deficiências identificadas no relatório de avaliação e transmitir esse plano de ação à Comissão e ao Conselho,

RECOMENDA:

Portugal deverá:

Autoridade de controlo da proteção de dados

1. Afetar à autoridade de proteção de dados recursos financeiros e humanos suficientes para que esta possa desempenhar todas as funções que lhe incumbem no âmbito do Sistema de Informação de Schengen II (SIS II) e do Sistema de Informação sobre Vistos (VIS), antecipando o futuro alargamento das suas competências;

2. A fim de garantir a plena independência dessa autoridade, conceder-lhe autonomia financeira para executar o seu orçamento anual e autonomia para recrutar pessoal, harmonizando, pelo menos, as normas que lhe são aplicáveis com as aplicáveis a outras autoridades independentes em Portugal;

3. Garantir que a autoridade de proteção de dados finaliza, sem demora, o procedimento de adoção dos relatórios elaborados na sequência da inspeção efetuada ao tratamento de dados pessoais no âmbito do SIS II;

4. Garantir que a autoridade de proteção de dados conclui, sem demora, a auditoria do VIS;

Direitos dos titulares dos dados

5. Assegurar que o sítio Web do Serviço de Estrangeiros e Fronteiras (SEF) mantém os titulares dos dados informados dos direitos que lhes assistem no que se refere ao SIS II;

6. Garantir que, na sequência da apresentação de um pedido de acesso a dados pessoais, os respetivos titulares são informados das categorias de dados efetivamente tratados no âmbito do SIS II;

7. Assegurar que os titulares de dados recebem informações claras quanto à identidade dos responsáveis pelo tratamento dos seus dados pessoais no âmbito da emissão de vistos Schengen;

Sistema de Informação sobre Vistos

8. Clarificar a situação quanto à responsabilidade pelo tratamento dos dados pessoais no âmbito do N.VIS, incluindo as aplicações utilizadas tanto pelo Ministério dos Negócios Estrangeiros (MNE) como pelo SEF e os respetivos centros de dados, nomeadamente esclarecendo o papel do MNE e clarificando a repartição das responsabilidades pelo tratamento dos dados pessoais entre o ministério e o SEF;

9. Garantir que o MNE leva a cabo atividades sistemáticas de supervisão que permitam avaliar adequadamente os diferentes aspetos do tratamento de dados pessoais por prestadores de serviços externos. Neste contexto, incentiva-se Portugal a alargar o questionário que o MNE envia aos prestadores de serviços externos, de modo a abranger mais pormenorizadamente os aspetos relativos à proteção de dados e a reforçar as atividades de supervisão do MNE quanto à proteção dos dados assegurada pelos mesmos ou pelo subcontratante, consoante o caso;

10. Estabelecer um procedimento que permita verificar as respostas positivas do SIS II no âmbito dos procedimentos de emissão de vistos;

11. Garantir a encriptação das senhas de todos os utilizadores do N.VIS;

12. Assegurar que o SEF e o MNE analisam com regularidade os ficheiros históricos, a fim de assegurar o controlo da proteção de dados;

13. Garantir que o MNE efetua regularmente o autocontrolo do tratamento dos dados pessoais na Rede de Pedidos de Vistos (RPV) e no respetivo centro de dados;

14. Assegurar que o MNE adota, sem demora, o plano de segurança para a RPV e o respetivo centro de dados;

15. Aplicar na íntegra a Decisão 2008/633/JAI do Conselho, de 23 de junho de 2008, relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades designadas dos Estados-Membros e por parte da Europol para efeitos de prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves, assegurando que o acesso aos dados N.VIS cumpre as exigências e os procedimentos aí estabelecidos;

16. Assegurar que os prestadores de serviços externos suprimem os dados pessoais dos requerentes armazenados nos seus sistemas dentro dos prazos fixados no anexo X, parte A, alínea d), do Código de Vistos, que impõe a supressão dos dados imediatamente após a sua transmissão ao consulado;

Sistema de Informação de Schengen II

17. Prever instalações de salvaguarda integral do N.SIS II, que disponham de todas as funcionalidades, nomeadamente a ligação à infraestrutura de comunicação s-TESTA;

18. Clarificar a repartição de responsabilidades entre as partes envolvidas no tratamento dos dados do N.SIS II, nomeadamente o responsável pelo tratamento de dados e as autoridades com acesso ao SIS.II (entidades utilizadoras), em termos de segurança informática, controlo e autocontrolo, por exemplo celebrando acordos entre os responsáveis pelo tratamento de dados e as autoridades que têm acesso ao SIS II;

19. Aplicar um sistema de gestão dos utilizadores que permita efetuar um autocontrolo eficaz, com base nos registos centrais do responsável pelo tratamento dos dados do N.SIS II, sem que seja necessário recorrer aos registos das entidades utilizadoras;

20. Assegurar que o SEF analisa regularmente os ficheiros históricos, a fim de assegurar o controlo da proteção de dados;

21. Assegurar que os ambientes informáticos dos utilizadores com direitos de acesso mais extensos ou que podem editar dados do N.SIS II (entre outros, os membros do gabinete SIRENE) estão virtual ou fisicamente isolados do acesso à Internet;

22. Assegurar que os responsáveis pelo tratamento dos dados encriptam os discos duros e bandas magnéticas de salvaguarda do N.SIS;

23. Garantir que os perfis dos utilizadores com direitos de acesso mais extensos ou que podem editar dados do N.SIS II (entre outros, os membros do gabinete SIRENE) são protegidos obrigatoriamente por um método de autenticação de dois fatores;

24. Assegurar que o SEF reforça as suas atividades de autocontrolo do tratamento de dados pessoais no N.SIS e efetua regularmente esse autocontrolo. Portugal é ainda incentivado a afetar ao SEF recursos financeiros e humanos suficientes para assegurar, de forma eficaz e contínua, as auditorias internas e a segurança informática, em particular provendo o cargo de responsável pela segurança informática do departamento de tecnologias da informação do SEF;

Sensibilização do público

25. Assegurar que o sítio Web do SEF disponibiliza ligações adequadas para o sítio Web da autoridade de proteção de dados.

Feito em Bruxelas, em

Pelo Conselho
O Presidente