



Bruxelas, 17 de junho de 2022  
(OR. en)

10396/22

---

---

Dossiê interinstitucional:  
2021/0224(NLE)

---

---

SCH-EVAL 83  
DATAPROTECT 197  
COMIX 324

## RESULTADOS DOS TRABALHOS

---

de: Secretariado-Geral do Conselho

data: 17 de junho de 2022

para: Delegações

---

n.º doc. ant.: 7788/22

---

Assunto: Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2020 relativa à aplicação pela **Áustria** 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 2020 relativa à aplicação pela Áustria do acervo de Schengen no domínio da proteção de dados, adotada pelo Conselho na sua reunião realizada a 17 de junho de 2022.

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 2020 relativa à aplicação pela Áustria 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<sup>1</sup>, nomeadamente o artigo 15.º,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

- (1) Em novembro de 2020, foi realizada uma avaliação de Schengen no domínio da proteção de dados em relação à Áustria. Na sequência dessa avaliação, foi adotado, mediante a Decisão de Execução C(2021) 9200 da Comissão, um relatório que inclui conclusões e apreciações, bem como uma lista das melhores práticas e das deficiências identificadas durante a avaliação.

---

<sup>1</sup> JO L 295 de 6.11.2013, p. 27.

- (2) Consideram-se boas práticas, em particular: que, desde a última avaliação, o pessoal da autoridade austríaca para a proteção de dados (APD) tenha sido reforçado e que continue a sê-lo, bem como o facto de o orçamento ter sido aumentado; os acordos entre o responsável pelo tratamento e o subcontratante em relação aos dados VIS preveem um elevado nível de proteção de dados e asseguram que todas as partes envolvidas no tratamento de dados VIS dispõem de garantias pertinentes em matéria de proteção de dados; a formação do pessoal em questões de proteção de dados relacionadas com o VIS pelo Ministério do Interior e pelo Ministério dos Assuntos Europeus e Internacionais; a abordagem multifacetada do Ministério dos Assuntos Europeus e Internacionais para auditar o processo de emissão de vistos; as informações fornecidas pela autoridade austríaca para a proteção de dados relativamente ao SIS II e ao VIS são muito pormenorizadas e facilmente acessíveis; os dossiês de informação sobre o SIS e o VIS no sítio Web do Ministério do Interior e o facto desta entidade responder aos pedidos de acesso relativos ao SIS II ou ao VIS num curto espaço de tempo.
- (3) Deverão ser formuladas recomendações sobre as medidas corretivas a tomar pela Áustria para suprir as deficiências identificadas durante a avaliação. Tendo em conta a importância de dar cumprimento ao acervo de Schengen em matéria de proteção de dados pessoais, deverá ser dada prioridade à execução das recomendações 1, 6, 7 e 13 constantes da presente decisão.
- (4) A presente decisão deverá ser transmitida ao Parlamento Europeu e aos parlamentos nacionais dos Estados-Membros. No prazo de três meses a contar da sua adoção, a Áustria 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, destinado a corrigir as deficiências identificadas no relatório de avaliação, e transmitir esse plano de ação à Comissão e ao Conselho,

RECOMENDA:

A Áustria deverá:

### **Legislação**

1. Aplicar o artigo 79.º do Regulamento Geral sobre a Proteção de Dados<sup>1</sup> e transpor o artigo 54.º da Diretiva (UE) 2016/680<sup>2</sup> para o direito nacional austríaco, a fim de prever o direito a um recurso judicial efetivo contra a decisão de um responsável pelo tratamento ou subcontratante que seja uma autoridade pública;

### **Entidade Responsável pela proteção de dados pessoais**

2. Estabelecer na lei as razões para a destituição do diretor e do diretor adjunto da autoridade austríaca para a proteção de dados, a fim de evitar o risco de cessação prematura das suas funções, exceto em caso de falta grave ou se já não preencherem as condições exigidas para o exercício das suas funções;
3. Assegurar que o perito em tecnologias da informação (TI) recém-recrutado pela autoridade austríaca para a proteção de dados e qualquer outro perito TI tenha ou venha a adquirir um conhecimento abrangente do Sistema de Informação de Schengen II (SIS II) e do Sistema de Informação sobre Vistos (VIS), bem como da gestão da segurança da informação, de modo a que esses peritos possam também participar ativamente nas atividades de supervisão do SIS e do VIS. Além disso, a autoridade austríaca para a proteção de dados (APD) deverá continuar a envolver peritos TI externos nas inspeções até poder cobrir todas as tarefas de inspeção relacionadas com as TI pelo seu próprio pessoal;

---

<sup>1</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

<sup>2</sup> Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

4. Assegurar que a autoridade austríaca para a proteção de dados (APD) efetue visitas de inspeção ao gabinete SIRENE, inspeções a algumas autoridades utilizadoras finais do sistema, como a polícia, bem como as monitorizações e análises regulares dos ficheiros de registo, a fim de cumprir as suas funções de controlo exaustivo do tratamento dos dados pessoais do SIS II;
5. Assegurar que as atividades de supervisão da autoridade austríaca para a proteção de dados (APD) em relação ao VIS abrangem também todos os aspetos de segurança, incluindo registos cronológicos, através de controlos regulares com base na análise dos ficheiros de registo, e que a autoridade austríaca para a proteção de dados inspecione exaustivamente as salas do servidor e inspecione também alguns outros utilizadores finais do sistema VIS, como a polícia;
6. Assegurar que a autoridade austríaca para a proteção de dados finalize a segunda auditoria ao N.VIS logo que a situação da COVID-19 o permitir;
7. Assegurar que a autoridade austríaca para a proteção de dados realize uma auditoria das operações de tratamento de dados no N.VIS, pelo menos, uma vez de quatro em quatro anos;

### **Sistema de Informação de Schengen**

8. Assegurar que todos os dispositivos que permitem o acesso aos dados do SIS II utilizem a autenticação bifatorial;
9. Assegurar que todos os documentos dos sistemas de gestão da segurança da informação existentes para ambos os centros de dados sejam revistos com maior frequência e que as normas utilizadas correspondam ainda ao estado da arte;
10. Assegurar que o plano de segurança para o SIS II seja revisto regularmente e atualizado sempre que necessário e que sejam estabelecidas medidas de segurança para garantir uma robustez duradoura, para além da confidencialidade, integridade e acessibilidade, em particular garantindo que o responsável pelo tratamento tenha em conta o desenvolvimento técnico para assegurar que as medidas de segurança adotadas continuem a cumprir esses objetivos;

11. Esclarecer se a autoridade de compensação central faz parte integrante do Ministério do Interior ou de um subcontratante externo de dados;
12. Assegurar que, no tratamento dos casos de usurpação de identidade, sejam introduzidas melhorias em relação às informações fornecidas ao titular dos dados e aos formulários de consentimento utilizados e que os formulários fornecidos ao titular dos dados incluam informações sobre os direitos dos titulares dos dados, os contactos do delegado para a proteção de dados, a base jurídica para o tratamento e informações sobre o período durante o qual os dados pessoais serão conservados;

### **Sistema de Informação sobre Vistos**

13. Assegurar que os registos de todas as operações de tratamento de dados no VIS sejam conservados a nível nacional, em conformidade com o artigo 34.º do Regulamento (CE) n.º 767/2008 (Regulamento VIS) (por um período de um ano após o período de conservação referido no artigo 23.º, n.º 1, do Regulamento VIS);

### **Sensibilização do público e direitos dos titulares dos dados**

14. Assegurar que o Ministério do Interior também disponibilize outras versões linguísticas (para além da língua alemã), por exemplo em inglês, do seu sítio Web relativo ao tratamento de dados do SIS II e do VIS e aos direitos conexos dos titulares dos dados, e torne mais fácil o acesso às informações do seu sítio Web sobre os direitos dos titulares dos dados em relação aos dados do SIS II e do VIS;
15. Assegurar que o Ministério do Interior disponibilize nos seus sítios Web formulários para o exercício dos direitos de acesso, correção e supressão, tanto em alemão como noutras línguas, por exemplo, em inglês;
16. Disponibilizar e tornar acessíveis às autoridades públicas versões em papel das brochuras informativas do SIS;

17. Assegurar que, a fim de reforçar os direitos dos titulares dos dados, o Ministério do Interior forneça uma tradução não oficial, por exemplo em inglês, das respostas aos titulares dos dados;
18. Assegurar que os sítios Web das Direções Provinciais de Polícia forneçam informações sobre o SIS II e o VIS, incluindo sobre o tratamento de dados pessoais, e que, nesses mesmos sítios Web, sejam apresentadas ligações para o sítio Web da autoridade austríaca para a proteção de dados (APD);
19. Assegurar que as informações sobre o tratamento de dados pessoais no VIS sejam fornecidas de forma facilmente acessível nos sítios Web do Ministério dos Assuntos Europeus e Internacionais e dos consulados e embaixadas e que esses sítios Web contenham hiperligações para o sítio Web da autoridade austríaca para a proteção de dados (APD);
20. Assegurar que a autoridade austríaca para a proteção de dados forneça as mesmas informações sobre a obrigação de o titular dos dados provar a sua identidade no seu sítio Web (em alemão e inglês), bem como nos formulários de pedido de acesso destinados ao titular dos dados;
21. Assegurar que a autoridade austríaca para a proteção de dados disponibilize no seu sítio Web (em alemão e inglês) formulários normalizados específicos para pedidos de retificação e apagamento relativos aos dados do SIS e do VIS;
22. Assegurar que a autoridade austríaca para a proteção de dados forneça informações sobre o prazo para a apresentação de uma queixa, conforme estabelecido no artigo 24.º, n.º 4, da Lei DP (Lei da proteção de dados), na versão inglesa do seu sítio Web.

Feito em Bruxelas, em

*Pelo Conselho*

*O Presidente*