Conselho da
União Europeia

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

**12468/19**

**Dossiê interinstitucional:**
**2019/0168(NLE)**

**SCH-EVAL 157**
**DATAPROTECT 216**
**COMIX 427**

**RESULTADOS DOS TRABALHOS**

| | |
|---|---|
| de: | Secretariado-Geral do Conselho |
| data: | 20 de setembro de 2019 |
| para: | Delegações |
| n.º doc. ant.: | 11904/19 |
| Assunto: | Decisão de Execução do Conselho que estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2018 relativa à aplicação pela **Lituânia** 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 relativa à aplicação pela Lituânia 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 Lituânia 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 Lituânia medidas corretivas para suprir as deficiências identificadas durante a avaliação de Schengen no domínio da proteção de dados efetuada em 2018. Na sequência dessa avaliação, foi adotado, pela Decisão de Execução C(2019) 5700 da Comissão, um relatório com as conclusões e apreciações, bem como uma lista das melhores práticas e das deficiências detetadas durante a avaliação.

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

(2) São consideradas boas práticas, nomeadamente, o facto de a Autoridade de Proteção de Dados (APD) prestar aconselhamento e orientação às pessoas que a contactam em vez de se limitar a reencaminhar os pedidos; a disponibilização de modelos de cartas para o exercício dos direitos dos titulares de dados a nível do Sistema de Informação de Schengen II (SIS II) e do Sistema de Informação sobre Vistos (VIS); as medidas de segurança aplicadas nas instalações do departamento de tecnologias da informação e comunicação (DTIC – que acolhe o N.VIS e o N.SIS) do Ministério do Interior (MI) são, em geral, de elevado nível, proporcionando um ambiente seguro para o armazenamento de dados e a prevenção de eventuais incidentes; a formação dos utilizadores finais do VIS, em especial do pessoal consular antes de ser destacado para embaixadas/consulados, está bem desenvolvida; existe um compromisso no que toca à formação e ao aperfeiçoamento do pessoal, em particular uma formação bem desenvolvida, inclusive em matéria de proteção de dados para os utilizadores finais do N.SIS e o pessoal do Gabinete SIRENE; as informações fornecidas pela APD no seu sítio Web no que se refere ao SIS II e ao VIS são bastante completas, úteis e com uma linguagem acessível (disponíveis em várias línguas); as brochuras da APD sobre "*Proteção de dados pessoais no âmbito do Sistema de Informação de Schengen*" e "*Proteção de dados pessoais no âmbito do Sistema de Informação sobre Vistos*" fornecem informações adequadas e acessíveis sobre o tratamento de dados em ambas as bases de dados e sobre os direitos conexos dos titulares dos dados bem como a forte participação da APD em muitas conferências, formações e outros eventos de sensibilização, incluindo para o pessoal encarregue do tratamento de dados no SIS II e no VIS.

(3) Tendo em conta a importância de dar cumprimento ao acervo de Schengen no domínio da proteção de dados, em especial para assegurar a total independência da APD, deverá ser dada prioridade à execução da recomendação 1.

(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, a Lituânia deverá, por força do artigo 16.º, n.º 1, do Regulamento (UE) n.º 1053/2013, estabelecer um plano de ação que enuncie todas as recomendações para corrigir quaisquer deficiências identificadas no relatório de avaliação e transmitir esse plano de ação à Comissão e ao Conselho,

RECOMENDA:

A Lituânia deverá:

**Autoridade de proteção de dados**

1. A fim de melhor garantir a plena independência da Inspeção Nacional de Proteção de Dados (a seguir designada por "APD"), abolir os requisitos que obrigam a que o plano de ação estratégico da APD seja aprovado pelo Ministro da Justiça e que este último seja consultado sobre o plano de ação anual antes que o diretor da APD possa aprová-lo; este aspeto é igualmente importante para assegurar que o processo orçamental não inclui qualquer risco de violação da independência da APD;

2. A fim garantir mais adequadamente a plena independência da APD, organizar as reuniões bilaterais realizadas regularmente entre o Ministro da Justiça e o diretor da APD de um modo que não implique qualquer risco de influência direta ou indireta do Governo na APD, que poderia prejudicar a independência da APD;

3. Abolir todos os elementos de responsabilização do diretor da APD em relação ao Governo e ao Ministro da Justiça suscetíveis de gerar o risco de influência direta ou indireta do Governo e do Ministro da Justiça, o que poderia prejudicar a independência da APD;

4. Assegurar que a APD controla mais frequentemente a legalidade do tratamento dos dados pessoais no SIS II;

5. Assegurar que, pelo menos de quatro em quatro anos, a APD realiza auditorias às operações de tratamento de dados no N.SIS;

6. Assegurar que a APD controla com maior frequência a legalidade do tratamento dos dados pessoais no VIS. A APD deve inspecionar igualmente as operações de tratamento de dados e a segurança dos dados dos prestadores de serviços externos quando inspeciona as embaixadas; esta possibilidade deve ser especificada no contrato entre o Ministério dos Negócios Estrangeiros (MNE) e os prestadores de serviços externos;

7. Assegurar que, pelo menos de quatro em quatro anos, a APD realiza auditorias às operações de tratamento de dados no N.VIS;

**Direitos dos titulares dos dados**

8. Assegurar que o prazo de 60 dias para responder aos pedidos dos titulares de dados no SIS II, previsto no artigo 41.º, n.º 6, do Regulamento SIS II, e no artigo 58.º, n.º 6, da Decisão SIS II, será respeitado até que o novo acervo do SIS[2] se torne plenamente aplicável (o mais tardar em 28 de dezembro de 2021) quando haja referências cruzadas para o prazo de resposta aos pedidos dos titulares de dados previsto no Regulamento Geral sobre a Proteção de Dados (RGPD)[3] (30 dias, com possibilidade de prorrogação por mais dois meses, se necessário);

9. Clarificar os procedimentos internos relativos à responsabilidade das autoridades envolvidas no tratamento dos direitos dos titulares de dados no SIS II; desta forma o pessoal também poderá saber a quem dirigir os pedidos;

---

[2] Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56) (ver, em especial, os artigos 66.º a 71.º); Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14) (ver, em especial, os artigos 51.º a 57.º).

[3] 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).

10. Assegurar que o Ministério do Interior é coerente nas respostas finais às pessoas que pretendem exercer os seus direitos de titulares de dados no SIS II, de modo a que sejam prestadas informações sobre o seu direito de recorrer à APD e os direitos de recurso para os tribunais;

11. Clarificar os procedimentos internos relativos à responsabilidade das autoridades envolvidas no tratamento dos direitos dos titulares de dados no VIS; desta forma o pessoal também poderá saber a quem dirigir os pedidos;

12. Assegurar que o Ministério do Interior é coerente nas respostas finais transmitidas às pessoas que pretendem exercer os seus direitos de titulares de dados no VIS, de modo a que sejam prestadas informações sobre o seu direito de recorrer à APD e os direitos de recurso para os tribunais;

**Sistema de Informação sobre Vistos**

13. Adotar as medidas necessárias para assegurar que os contratos entre o MNE e os prestadores de serviços externos regulam a forma como a APD lituana pode participar nas inspeções realizadas pelas embaixadas/consulados e pelo MNE;

14. Melhorar o autocontrolo através da verificação proativa e regular dos registos, a fim de controlar a legalidade do tratamento dos dados pessoais no VIS. O Ministério do Interior deve continuar a desenvolver o sistema SIEM de controlo automático dos registos;

15. Assegurar a participação mais ativa do encarregado da proteção de dados (EPD) do MNE no desenvolvimento e na prestação de formação sobre proteção de dados ao pessoal do MNE, incluindo o pessoal destacado em embaixadas/consulados;

**Sistema de Informação de Schengen II**

16. Suprimir a possibilidade de um utilizador final iniciar uma sessão no N.SIS através do programa de navegação "POLIS" com vários dispositivos em simultâneo;

17. Assegurar que serão introduzidos cartões inteligentes para o acesso aos terminais informáticos dos utilizadores do N.SIS na polícia, a fim de aumentar o nível e os padrões de segurança;

18. Assegurar que as medidas técnicas vigentes para impedir a utilização de chaves USB nos terminais informáticos do Gabinete SIRENE são integralmente aplicadas e controladas de forma regular;

19. Melhorar o autocontrolo através da verificação proativa e regular dos registos dos utilizadores finais do SIS II pertencentes a todas as autoridades em causa, a fim de controlar a legalidade do tratamento dos dados pessoais no SIS II. O Ministério do Interior deve continuar a desenvolver o sistema SIEM de controlo automático dos registos;

20. Assegurar que a sensibilização para a proteção de dados do pessoal em relação ao tratamento dos dados do SIS II e do VIS é reforçada através de sessões de formação de atualização periódica;

21. Assegurar que a formação e a sensibilização do pessoal com acesso ao N.SIS serão domínios que os encarregados da proteção de dados do Ministério do Interior irão liderar, garantindo assim uma estrutura e um planeamento continuados para o desenvolvimento do pessoal;

**Sensibilização do público**

22. Assegurar a atualização regular das ligações no sítio Web da APD respeitantes ao SIS II e ao VIS;

23. Assegurar que os sítios Web das entidades que têm contactos com sítios Web nacionais de outros países, como o Ministério do Interior, a Polícia, o Serviço da Guarda de Fronteiras, o MNE e os serviços consulares, disponibilizam informações acessíveis e claras também em inglês sobre o SIS II, o VIS e os direitos conexos dos titulares de dados;

24. Assegurar que, quando os sítios Web fornecem informações em inglês sobre o SIS II, o VIS e os direitos conexos dos titulares de dados, essas informações sejam mais fáceis de encontrar;

25. Assegurar a coerência das informações sobre o exercício dos direitos dos titulares de dados em relação aos N.SIS II e ao VIS que figuram nos sítios Web das instituições que trabalham com estes sistemas;

26. Acrescentar informações sobre o tratamento de dados e os direitos conexos dos titulares de dados relativamente ao VIS no portal EPM através do qual as pessoas singulares fornecem os seus dados para os pedidos de visto.

Feito em Bruxelas, em

*Pelo Conselho*
*O Presidente*