DECISÃO DA COMISSÃO

de 4 de Maio de 2010

relativa ao plano de segurança para o funcionamento do Sistema de Informação sobre Vistos

(2010/260/UE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de Julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração («Regulamento VIS») [1], nomeadamente o artigo 32.º, n.º 4,

Considerando o seguinte:

(1) O artigo 32.º, n.º 3, do Regulamento (CE) n.º 767/2008 determina que a autoridade de gestão deve tomar as medidas necessárias para atingir os objectivos em matéria de segurança relativamente ao funcionamento do VIS previstos no n.º 2 do mesmo artigo, incluindo a adopção do plano de segurança.

(2) O artigo 26.º, n.º 4, do Regulamento (CE) n.º 767/2008 prevê que, durante um período transitório antes de a autoridade de gestão assumir as suas funções, a Comissão é responsável pela gestão operacional do VIS.

(3) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho [2] aplica-se ao tratamento dos dados pessoais a realizar pela Comissão no contexto das suas responsabilidades de gestão operacional do VIS.

(4) O artigo 26.º, n.º 7, do Regulamento (CE) n.º 767/2008 determina que, no caso de a Comissão delegar as suas responsabilidades durante o período transitório antes de a autoridade de gestão assumir as suas funções, deve assegurar que essa delegação não tem repercussões negativas em relação a qualquer mecanismo de controlo eficaz, instituído ao abrigo do direito da União, quer se trate do Tribunal de Justiça, do Tribunal de Contas ou da Autoridade Europeia para a Protecção de Dados.

(5) A autoridade de gestão deve estabelecer o seu próprio plano de segurança relativo ao VIS quando assumir as suas funções.

(6) A Decisão 2008/602/CE da Comissão, de 17 de Junho de 2008, que estabelece a arquitectura física e os requisitos das interfaces nacionais e da infra-estrutura de comunicação entre o VIS Central e as interfaces nacionais durante a fase de desenvolvimento [3], definiu as exigências aplicáveis à rede do VIS em termos de serviços de segurança.

(7) O artigo 27.º do Regulamento (CE) n.º 767/2008 prevê que o VIS Central principal, que executa funções de supervisão técnica e administração, está localizado em Estrasburgo (França) e que o VIS Central de salvaguarda, capaz de assegurar todas as funcionalidades do VIS Central principal em caso de falha deste último, está localizado em Sankt Johann im Pongau (Áustria).

(8) Devem ser definidos os papéis dos responsáveis pela segurança a fim de assegurar uma resposta rápida e eficiente a quaisquer incidentes de segurança e que estes são objecto de relatórios.

(9) Deve ser criada uma política de segurança que descreva todos os aspectos técnicos e organizacionais em conformidade com as disposições da presente decisão.

(10) Devem ser tomadas medidas para assegurar o nível de segurança adequado para o funcionamento do VIS,

ADOPTOU A PRESENTE DECISÃO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objecto

A presente decisão estabelece a organização e as medidas de segurança (plano de segurança) na acepção do artigo 32.º, n.º 3, do Regulamento (CE) n.º 767/2008.

CAPÍTULO II

ORGANIZAÇÃO, RESPONSABILIDADES E GESTÃO DE INCIDENTES

Artigo 2.º

Tarefas da Comissão

1. A Comissão aplica e controla a eficácia das medidas de segurança para o VIS Central e para a infra-estrutura de comunicação referida na presente decisão.

[1] JO L 218 de 13.8.2008, p. 60.
[2] JO L 8 de 12.1.2001, p. 1.
[3] JO L 194 de 23.7.2008, p. 3.

2. A Comissão designa, de entre os seus funcionários, um responsável pela segurança do sistema. O responsável pela segurança do sistema é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão. As tarefas do responsável pela segurança do sistema incluem, em especial:

a) Preparar, actualizar e rever a política de segurança, em conformidade com o artigo 7.º da presente decisão;

b) Controlar a eficácia da aplicação dos procedimentos de segurança do VIS Central e da infra-estrutura de comunicação;

c) Contribuir para a elaboração do relatório de segurança referido no artigo 50.º, n.os 3 e 4, do Regulamento (CE) n.º 767/2008;

d) Executar tarefas de coordenação e assistência nas verificações e auditorias realizadas pela Autoridade Europeia para a Protecção de Dados referidas no artigo 42.º do Regulamento (CE) n.º 767/2008;

e) Verificar se a presente decisão e a política de segurança são correcta e integralmente aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão e funcionamento do VIS;

f) Manter uma lista dos pontos de contacto nacionais únicos para segurança do VIS e partilhá-la com os responsáveis locais pela segurança do VIS Central e da infra-estrutura de comunicação.

Artigo 3.º

Responsável local pela segurança do VIS Central

1. Sem prejuízo do disposto no artigo 8.º, a Comissão designa, de entre os seus funcionários, um responsável local pela segurança do VIS Central. Devem ser evitados os conflitos de interesses entre as funções de responsável local pela segurança e quaisquer outras funções oficiais. O responsável local pela segurança do VIS Central é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão.

2. O responsável local pela segurança do VIS Central assegura que as medidas de segurança referidas na presente decisão são aplicadas e que os procedimentos de segurança são respeitados no VIS Central principal. No que diz respeito ao VIS Central de salvaguarda, o responsável local pela segurança do VIS Central assegura que as medidas de segurança referidas na presente decisão são aplicadas, com excepção das referidas no artigo 10.º, e que os respectivos procedimentos de segurança são respeitados.

3. O responsável local pela segurança do VIS Central pode delegar algumas das suas tarefas no pessoal subordinado. Devem ser evitados os conflitos de interesses entre as funções inerentes à execução destas tarefas e quaisquer outras funções oficiais. Através de um número de telefone e endereço de contacto únicos, será possível contactar a qualquer momento o responsável local pela segurança ou o seu subordinado de serviço.

4. O responsável local pela segurança do VIS Central executa as tarefas inerentes às medidas de segurança a adoptar nos sistemas VIS Centrais principal e de salvaguarda, dentro dos limites do n.º 1, incluindo, em especial:

a) Realizar as tarefas operacionais de segurança local, incluindo auditorias à barreira de segurança (*firewall*), testes regulares de segurança, auditorias e relatórios;

b) Verificar a eficácia do plano de continuidade das actividades e assegurar a realização de exercícios regulares;

c) Recolher elementos de prova e comunicar ao responsável pela segurança do sistema qualquer incidente que possa ter impacto na segurança do VIS Central ou da infra-estrutura de comunicação;

d) Informar o responsável pela segurança do sistema no caso de a política de segurança dever ser alterada;

e) Verificar se a presente decisão e a política de segurança são aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão e funcionamento do VIS Central;

f) Assegurar que o pessoal está consciente das suas obrigações e verificar a aplicação da política de segurança;

g) Acompanhar os desenvolvimentos em matéria de segurança das TI e assegurar que o pessoal dispõe da formação adequada;

h) Preparar a informação e opções subjacentes à definição, actualização e revisão da política de segurança nos termos do artigo 7.º.

Artigo 4.º

Responsável local pela segurança da infra-estrutura de comunicação

1. Sem prejuízo do disposto no artigo 8.º, a Comissão designa, de entre os seus funcionários, um responsável local pela segurança da infra-estrutura de comunicação. Devem ser evitados os conflitos de interesses entre as funções de responsável local pela segurança e quaisquer outras funções oficiais. O responsável local pela segurança da infra-estrutura de comunicação é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão.

2. O responsável local pela segurança da infra-estrutura de comunicação verifica o funcionamento da infra-estrutura de comunicação e assegura que as medidas de segurança são aplicadas e os procedimentos de segurança respeitados.

3. O responsável local pela segurança da infra-estrutura de comunicação pode delegar algumas das suas tarefas no pessoal subordinado. Devem ser evitados os conflitos de interesses entre as funções inerentes à execução destas tarefas e quaisquer outras funções oficiais. Através de um número de telefone e endereço de contacto únicos, será possível contactar a qualquer momento o responsável local pela segurança ou o seu subordinado de serviço.

4. O responsável local pela segurança da infra-estrutura de comunicação executa as tarefas inerentes às medidas de segurança relativas à infra-estrutura de comunicação, incluindo, em especial:

a) Realizar todas as tarefas operacionais de segurança relativas à infra-estrutura de comunicação, incluindo auditorias à barreira de segurança (*firewall*), testes regulares de segurança, auditorias e relatórios;

b) Verificar a eficácia do plano de continuidade das actividades e assegurar a realização de exercícios regulares;

c) Recolher elementos de prova e comunicar ao responsável pela segurança do sistema qualquer incidente que possa ter impacto na segurança da infra-estrutura de comunicação, do VIS Central ou dos sistemas nacionais;

d) Informar o responsável pela segurança do sistema no caso de a política de segurança dever ser alterada;

e) Verificar se a presente decisão e a política de segurança são aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão da infra-estrutura de comunicação;

f) Assegurar que o pessoal está consciente das suas obrigações e verificar a aplicação da política de segurança;

g) Acompanhar os desenvolvimentos em matéria de segurança das TI e assegurar que o pessoal dispõe da formação adequada;

h) Preparar a informação e opções subjacentes à definição, actualização e revisão da política de segurança nos termos do artigo 7.º.

Artigo 5.º

Incidentes de segurança

1. Qualquer acontecimento que tenha ou possa ter impacto na segurança do funcionamento do VIS e que possa causar-lhe danos é considerado um incidente de segurança, nomeadamente quando possa ter havido acesso aos dados ou quando a disponibilidade, integridade e confidencialidade dos dados tenham ou possam ter sido postas em causa.

2. A política de segurança define procedimentos de recuperação em caso de incidente. Os incidentes de segurança são geridos por forma a assegurar uma resposta rápida, eficaz e adequada, em conformidade com a política de segurança.

3. As informações relativas a um incidente de segurança que tenha ou possa ter impacto no funcionamento do VIS num Estado-Membro ou na disponibilidade, integridade e confidencialidade dos dados VIS registados por um Estado-Membro são facultadas ao Estado-Membro em causa. Os incidentes de segurança são comunicados ao responsável pela protecção de dados da Comissão.

Artigo 6.º

Gestão de incidentes

1. Sempre que necessário, Todos os membros do pessoal e contratantes envolvidos no desenvolvimento, gestão ou funcionamento do VIS devem registar e comunicar ao responsável pela segurança do sistema ou ao responsável local pela segurança do VIS Central ou ao responsável local pela segurança da infra-estrutura de comunicação, consoante o caso, quaisquer constatações ou suspeitas de problemas de segurança no funcionamento do VIS.

2. Caso detecte qualquer incidente que tenha ou possa ter impacto na segurança do funcionamento do VIS, o responsável local pela segurança do VIS Central ou o responsável local pela segurança da infra-estrutura de comunicação deve informar o mais rapidamente possível o responsável pela segurança do sistema e, se necessário, o ponto de contacto nacional único para a segurança do VIS, quando este existir no Estado-Membro em questão, devendo fazê-lo por escrito ou, em caso de extrema urgência, através de outros canais de comunicação. O relatório deve conter a descrição do incidente de segurança, o nível de risco, as eventuais consequências e as medidas que foram ou devem ser adoptadas para atenuar o risco.

3. Quaisquer elementos relativos ao incidente de segurança são imediatamente salvaguardados pelo responsável local pela segurança do VIS Central ou pelo responsável local pela segurança da infra-estrutura de comunicação, consoante o caso. Na medida do possível, nos termos das disposições aplicáveis à protecção dos dados, essas provas são disponibilizadas ao responsável pela segurança do sistema, a seu pedido.

4. São criados mecanismos de comunicação que assegurem a circulação da informação sobre os resultados quando o incidente tiver sido tratado e terminado.

CAPÍTULO III

MEDIDAS DE SEGURANÇA

Artigo 7.º

Política de segurança

1. O director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança estabelece, actualiza e revê regularmente uma política de segurança vinculativa, em conformidade com a presente decisão. A política de segurança prevê, de forma pormenorizada, os procedimentos e medidas de protecção contra ameaças à disponibilidade, integridade e confidencialidade do VIS, incluindo um plano de emergência, a fim de assegurar o nível adequado de segurança, conforme previsto na presente decisão. A política de segurança deve respeitar a presente decisão.

2. A política de segurança é baseada numa avaliação dos riscos. As medidas descritas na política de segurança devem ser proporcionais aos riscos identificados.

3. A avaliação dos riscos e da política de segurança serão actualizadas sempre que a evolução tecnológica, a identificação de novas ameaças ou quaisquer outras circunstâncias o tornem necessário. Em todo o caso, a política de segurança é revista numa base anual, para assegurar que continua a responder adequadamente à última avaliação dos riscos, a quaisquer outras evoluções tecnológicas ou ameaças recentemente identificadas ou a outras circunstâncias relevantes.

4. A política de segurança é elaborada pelo responsável pela segurança do sistema, em coordenação com o responsável local pela segurança do VIS Central e o responsável local pela segurança da infra-estrutura de comunicação.

Artigo 8.º

Aplicação das medidas de segurança

1. A realização das tarefas e a aplicação dos requisitos estabelecidos na presente decisão e na política de segurança, incluindo a tarefa de designar um responsável local pela segurança, pode ser objecto de subcontratação ou confiada a organismos privados ou públicos.

2. Neste caso, a Comissão deve assegurar, através de acordos juridicamente vinculativos, que os requisitos estabelecidos na presente decisão e na política de segurança são integralmente respeitados. Em caso de delegação ou subcontratação da tarefa de designar um responsável local pela segurança, a Comissão deve assegurar, através de acordos juridicamente vinculativos, que será consultada relativamente à pessoa a designar para esta função.

Artigo 9.º

Controlo do acesso às instalações

1. Devem ser utilizados perímetros de segurança com barreiras e controlos de entrada adequados para proteger as instalações onde se realiza o tratamento de dados.

2. Nos perímetros de segurança devem ser definidas áreas seguras para proteger os componentes físicos (bens), incluindo o equipamento informático, os suportes de dados e consolas, os planos e outros documentos sobre o VIS, bem como os gabinetes e outros locais de trabalho do pessoal envolvido no funcionamento do VIS. Estas áreas seguras devem ser protegidas por controlos de entrada adequados, para assegurar que só o pessoal autorizado pode ter acesso. O trabalho nas áreas seguras deve estar sujeito a regras de segurança pormenorizadas estabelecidas na política de segurança.

3. Deve ser prevista e instalada a segurança física dos gabinetes, salas e instalações. Os pontos de acesso, como as áreas de cargas e descargas e outros pontos onde possam entrar nas instalações pessoas não autorizadas, devem ser controlados e, se possível, isolados das instalações de tratamento dos dados, para evitar o acesso não autorizado.

4. Deve ser concebida uma protecção física dos perímetros de segurança contra danos resultantes de catástrofes naturais ou de origem humana e aplicada proporcionalmente ao respectivo risco.

5. O equipamento deve ser protegido contra as ameaças físicas e ambientais, bem como contra a possibilidade de acesso não autorizado.

6. Se a Comissão dispuser de tal informação, deve acrescentar à lista referida no artigo 2.º, n.º 2, alínea f), um ponto de contacto único para acompanhar a aplicação do disposto no presente artigo nas instalações onde está localizado o VIS Central de salvaguarda.

Artigo 10.º

Controlo dos suportes de dados e bens

1. Os suportes móveis que contenham dados devem ser protegidos contra acessos não autorizados, utilização indevida ou corrupção dos dados, devendo a sua legibilidade ser assegurada ao longo de toda a vida útil dos dados.

2. Quando já não forem necessários, os suportes devem ser eliminados de forma segura, segundo os procedimentos pormenorizados estabelecidos na política de segurança.

3. Devem estar disponíveis inventários com informação sobre a localização dos dados arquivados, o período de conservação aplicável e as autorizações de acesso.

4. Todos os elementos importantes do VIS Central e da infra-estrutura de comunicação devem ser identificados, para que possam ser protegidos de acordo com a sua importância. Deve ser mantido um registo actualizado do equipamento informático relevante.

5. A documentação actualizada relativa ao VIS Central e à infra-estrutura de comunicação deve estar disponível. Esta documentação deve ser protegida contra acessos não autorizados.

Artigo 11.º

Controlo do arquivo de dados

1. São tomadas medidas adequadas para assegurar o arquivamento adequado da informação e a sua protecção contra acessos não autorizados.

2. Todos os equipamentos que contenham dados arquivados devem ser verificados para assegurar que os dados sensíveis foram retirados ou integralmente apagados antes da sua remoção, ou devem ser destruídos de forma segura.

Artigo 12.º

Controlo de palavras-passe

1. Todas as palavras-passe são mantidas em segurança e tratadas confidencialmente. Quando haja suspeitas de que uma palavra-passe foi divulgada, esta deve ser imediatamente alterada ou a conta do utilizador desactivada. Os nomes de utilizador devem ser únicos e individuais.

2. Os procedimentos para iniciar e terminar uma sessão são definidos na política de segurança para impedir quaisquer acessos não autorizados.

Artigo 13.º

Controlo de acessos

1. A política de rança estabelece um procedimento de registo e supressão do registo do pessoal em actividade, destinado a conceder e revogar o acesso ao equipamento e ao sistema do VIS Central para efeitos de gestão operacional. A atribuição e utilização das credenciais de acesso adequadas (palavras-passe ou outros meios adequados) são controladas através de um processo de gestão formal, em conformidade com a política de segurança.

2. O acesso ao equipamento e ao *software* do VIS Central deve:

i) Ser limitado às pessoas autorizadas;

ii) Ser limitado aos casos em que possa ser identificado um objectivo legítimo em conformidade com os artigos 42.º e 50.º, n.º 2, do Regulamento (CE) n.º 767/2008;

iii) Não exceder a duração e âmbito necessários ao objectivo do acesso; e

iv) Ter lugar apenas nos termos da política de controlo de acesso a definir na política de segurança.

3. Só as consolas e *software* autorizados pelo responsável local pela segurança do VIS Central podem ser utilizados no VIS Central. A utilização de funções do sistema susceptíveis de ultrapassar os controlos do sistema e das aplicações é restringida e controlada. Devem ser criados procedimentos de controlo da instalação de *software*.

Artigo 14.º

Controlo da comunicação

A infra-estrutura de comunicação deve ser verificada a fim de assegurar a disponibilidade, integridade e confidencialidade dos intercâmbios de informações. Devem ser utilizados meios criptográficos para proteger os dados transmitidos através da infra-estrutura de comunicação.

Artigo 15.º

Controlo do registo de dados

As contas das pessoas autorizadas a aceder ao *software* VIS do VIS Central são controladas pelo responsável local pela segurança do VIS Central. A utilização dessas contas, incluindo o tempo e a identidade do utilizador, é registada.

Artigo 16.º

Controlo do transporte

1. São definidas medidas adequadas na política de segurança para impedir a leitura, cópia, alteração ou supressão não autorizada dos dados pessoais durante a transmissão de ou para o VIS ou durante o transporte dos suportes de dados. A política de segurança deve incluir disposições sobre os tipos admissíveis de envio ou transporte, bem como sobre a responsabilidade pelos procedimentos relativos ao transporte desses elementos e à sua chegada ao local de destino. Os suportes de dados não devem conter quaisquer dados para além dos que devem ser enviados.

2. Os serviços prestados por terceiros que impliquem o acesso, comunicação ou gestão das instalações de tratamento de dados ou o fornecimento de bens ou serviços a essas instalações, devem incluir controlos de segurança integrados adequados.

Artigo 17.º

Segurança da infra-estrutura de comunicação

1. A infra-estrutura de comunicação deve ser adequadamente gerida e controlada, a fim de a proteger contra as ameaças e garantir a segurança da própria infra-estrutura de comunicação e do VIS Central, incluindo a dos dados transmitidos por essa via.

2. As características de segurança, os níveis de serviço e os requisitos de gestão de todos os serviços de rede devem ser identificados no acordo de serviços de rede celebrado com o fornecedor de serviços.

3. Além da protecção dos pontos de acesso ao VIS, qualquer serviço adicional utilizado pela infra-estrutura de comunicação deve igualmente ser protegido. As medidas adequadas são definidas na política de segurança.

Artigo 18.º

Acompanhamento

1. Os registos da informação referida no artigo 34.º, n.º 1, do Regulamento (CE) n.º 767/2008, relativa a todos os acessos e operações de tratamento de dados no VIS Central, são conservados em segurança e estão acessíveis nas instalações onde estão localizados os VIS Centrais principal e de salvaguarda durante o período referido no artigo 34.º, n.º 2, do Regulamento (CE) n.º 767/2008.

2. Os procedimentos de controlo da utilização das instalações de tratamento de informação ou das suas deficiências são definidos na política de segurança e os resultados das actividades de controlo devem ser avaliados regularmente. Se necessário, são tomadas as medidas adequadas.

3. Os registos e respectivos suportes são protegidos contra a manipulação indevida e o acesso não autorizado, para respeitarem os requisitos relativos à recolha e ao período de conservação dos dados.

Artigo 19.º

Medidas criptográficas

São utilizadas medidas criptográficas adequadas para a protecção da informação. A sua utilização, objectivos e condições, devem ser previamente aprovados pelo responsável pela segurança do sistema.

CAPÍTULO IV

SEGURANÇA DOS RECURSOS HUMANOS

Artigo 20.º

Perfis dos membros do pessoal

1. A política de segurança define as funções e responsabilidades das pessoas autorizadas a aceder ao VIS, incluindo a infra-estrutura de comunicação.

2. Os papéis e responsabilidades a nível de segurança do pessoal da Comissão, dos contratantes e do pessoal implicado na gestão operacional são definidos, registados e comunicados às pessoas em causa. A descrição de funções e os objectivos definem os papéis e responsabilidades do pessoal da Comissão; contratos ou acordos de nível de serviço definem-nos quanto aos contratantes.

3. São celebrados compromissos de confidencialidade e sigilo com todas as pessoas não abrangidas pelas regras da função pública da União Europeia ou dos Estados-Membros. O pessoal que trabalhe com dados do VIS deve ter a necessária autorização ou certificação, em conformidade com os procedimentos pormenorizados a estabelecer na política de segurança.

Artigo 21.º

Informação ao pessoal

1. Todos os membros do pessoal e, quando aplicável, os contratantes, recebem formação adequada sobre sensibilização para a segurança, requisitos legais, políticas e procedimentos, na medida em que as suas funções o exijam.

2. Relativamente à cessação da relação laboral ou do contrato, a política de segurança define as responsabilidades inerentes à mudança ou cessação de emprego, bem como os procedimentos para gerir a devolução dos bens e a supressão dos direitos de acesso.

CAPÍTULO V

DISPOSIÇÃO FINAL

Artigo 22.º

Aplicabilidade

1. A presente decisão é aplicável a partir da data determinada pela Comissão nos termos do artigo 48.º, n.º 1, do Regulamento (CE) n.º 767/2008.

2. A presente decisão caduca quando a autoridade de gestão assumir funções.

Feito em Bruxelas, em 4 de Maio de 2010.

Pela Comissão

O Presidente

José Manuel BARROSO