

II

(Actos não legislativos)

REGULAMENTOS

REGULAMENTO DE EXECUÇÃO (UE) N.º 1179/2011 DA COMISSÃO

de 17 de Novembro de 2011

que estabelece as especificações técnicas dos sistemas de recolha por via electrónica, nos termos do Regulamento (UE) n.º 211/2011 do Parlamento Europeu e do Conselho sobre a iniciativa de cidadania

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) n.º 211/2011 do Parlamento Europeu e do Conselho, de 16 de Fevereiro de 2011, sobre a iniciativa de cidadania⁽¹⁾, nomeadamente o seu artigo 6.º, n.º 5,

Após consulta da Autoridade Europeia para a Protecção de Dados,

Considerando o seguinte:

- (1) O Regulamento (UE) n.º 211/2011 estabelece que, nos casos em que as declarações de apoio são recolhidas por via electrónica, o sistema utilizado para o efeito deve satisfazer determinadas condições técnicas e de segurança e deve ser certificado pela autoridade competente do Estado-Membro em causa.
- (2) Um sistema de recolha por via electrónica, na acepção do Regulamento (UE) n.º 211/2011, consiste num sistema de informação, composto por *software*, *hardware*, ambiente de alojamento, processos específicos desta actividade e pessoal, com vista a proceder à recolha por via electrónica de declarações de apoio.
- (3) O Regulamento (UE) n.º 211/2011 define os requisitos que os sistemas de recolha por via electrónica devem satisfazer para serem certificados e estabelece que a Comissão deve adoptar especificações técnicas para a aplicação desses requisitos.
- (4) O projecto Top 10 2010 do OWASP (*Open Web Application Security Project*) oferece uma panorâmica dos riscos mais críticos, em termos de segurança, das aplicações *web* e das ferramentas para combater esses riscos; as especificações técnicas foram, pois, elaboradas com base nos resultados do referido projecto.
- (5) A aplicação das especificações técnicas pelos organizadores deve ser de molde a garantir a certificação, pela autoridade competente de cada Estado-Membro, dos sistemas de recolha por via electrónica e a contribuir para assegurar que são postas em prática as adequadas medidas técnicas e organizativas necessárias para dar cumprimento às obrigações impostas pela Directiva 95/46/CE do Parlamento Europeu e do Conselho⁽²⁾ no que respeita à segurança das actividades de tratamento de dados, tanto na fase de concepção do sistema de tratamento de dados como no decurso do tratamento propriamente dito, a fim de preservar a segurança e, desse modo, impedir qualquer tratamento não autorizado e proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, ou a divulgação ou acesso não autorizados.
- (6) O processo de certificação deve ser facilitado pela utilização, pelos organizadores, do *software* disponibilizado pela Comissão nos termos do artigo 6.º, n.º 2, do Regulamento (UE) n.º 211/2011.
- (7) Os organizadores de iniciativas de cidadania, enquanto responsáveis pelo tratamento dos dados, devem, ao proceder à recolha de declarações de apoio por via electrónica, aplicar as especificações técnicas definidas no presente regulamento, a fim de garantir a protecção dos dados pessoais a tratar. Nos casos em que o tratamento é efectuado por uma entidade especializada, os organizadores devem assegurar que essa entidade actua apenas mediante instruções dos organizadores e que aplica as especificações técnicas definidas no presente regulamento.
- (8) O presente regulamento respeita os direitos fundamentais e observa os princípios consagrados na Carta dos Direitos Fundamentais da União Europeia, nomeadamente o seu artigo 8.º, que dispõe que todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
- (9) As medidas previstas no presente regulamento são conformes com o parecer do comité instituído nos termos do artigo 20.º do Regulamento (UE) n.º 211/2011,

⁽¹⁾ JO L 65 de 11.3.2011, p. 1.

⁽²⁾ JO L 281 de 23.11.1995, p. 31.

ADOPTOU O PRESENTE REGULAMENTO:

Artigo 1.º

As especificações técnicas a que se refere o artigo 6.º, n.º 5, do Regulamento (UE) n.º 211/2011 constam do anexo.

Artigo 2.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 17 de Novembro de 2011.

Pela Comissão
O Presidente
José Manuel BARROSO

ANEXO

1. ESPECIFICAÇÕES TÉCNICAS COM VISTA À APLICAÇÃO DO ARTIGO 6.º, N.º 4, ALÍNEA a), DO REGULAMENTO (UE) N.º 211/2011

A fim de impedir a apresentação automatizada de declarações de apoio com recurso ao sistema, o subscritor é submetido a um processo de verificação adequado, conforme com a prática comum, antes de apresentar a sua declaração de apoio. Um processo de verificação possível é a utilização de um *captcha* forte.

2. ESPECIFICAÇÕES TÉCNICAS DESTINADAS À APLICAÇÃO DO ARTIGO 6.º, N.º 4, ALÍNEA b), DO REGULAMENTO (UE) N.º 211/2011

Normas de garantia da informação

- 2.1. Os organizadores fornecem documentação comprovativa de que preenchem os requisitos da norma ISO/IEC 27001, ainda que não a tenham adoptado. Para o efeito, terão:

- a) Realizado uma avaliação exaustiva dos riscos que identifique o âmbito de aplicação do sistema, assinalo o impacto na actividade em caso de várias violações da garantia da informação, enumere as ameaças e vulnerabilidades do sistema de informação, produza um documento de análise de riscos onde se enumerem igualmente contramedidas para evitar tais ameaças, bem como medidas correctivas a tomar caso a ameaça se concretize, e, por último, apresente uma lista hierarquizada de melhorias a introduzir;
- b) Formulado e aplicado medidas para tratar os riscos relacionados com a protecção dos dados pessoais e a protecção da vida familiar e privada, bem como medidas a tomar em caso de materialização de um risco;
- c) Identificado os riscos residuais por escrito;
- d) Assegurado os necessários meios organizacionais para receber informações de retorno em relação a novas ameaças e a melhorias em matéria de segurança.

- 2.2. Os organizadores seleccionam os controlos de segurança, com base na análise de riscos prevista no ponto 2.1, alínea a), de entre as seguintes normas;

(1) ISO/IEC 27002 ou

(2) «Princípios de boas práticas» do Fórum sobre a Segurança da Informação

para lidar com as seguintes questões:

- a) Avaliações de risco (recomenda-se a norma ISO/IEC 27005 ou outra metodologia de avaliação de riscos específica e adequada);
- b) Segurança física e ambiental;
- c) Segurança dos recursos humanos;
- d) Gestão de comunicações e operações;
- e) Medidas normalizadas de controlo do acesso, para além das previstas no presente regulamento de execução;
- f) Aquisição, desenvolvimento e manutenção dos sistemas de informação;
- g) Gestão de incidentes no domínio da segurança das informações;
- h) Medidas para corrigir e mitigar violações dos sistemas de informação susceptíveis de causar a destruição, a perda acidental, a alteração, ou a divulgação ou acesso não autorizados dos dados pessoais a tratar;
- i) Conformidade;
- j) Segurança de redes informáticas (recomenda-se a norma ISO/IEC 27033 ou os referidos «Princípios de boas práticas»).

A aplicação destas normas pode cingir-se às partes da organização que são relevantes para o sistema de recolha por via electrónica. Por exemplo, a segurança dos recursos humanos pode limitar-se a quaisquer elementos do pessoal com acesso físico ou em rede ao sistema de recolha por via electrónica e a segurança física e ambiental pode limitar-se ao(s) edifício(s) onde o sistema se encontra alojado.

Requisitos funcionais

- 2.3. O sistema de recolha por via electrónica consiste numa aplicação com base na *web* criada para efeitos de recolha de declarações de apoio a iniciativas de cidadania individuais.
- 2.4. Se a administração do sistema implica diferentes funções, são estabelecidos diferentes níveis de controlo do acesso, segundo o princípio do «privilégio mínimo».
- 2.5. Os elementos acessíveis ao público são claramente separados dos elementos destinados a fins de administração. A leitura da informação disponível na zona pública do sistema, incluindo informações sobre a iniciativa e o formulário da declaração de apoio por via electrónica, não será dificultada por nenhum controlo do acesso. Só é possível subscrever a iniciativa nessa zona pública do sistema.
- 2.6. O sistema detecta e impede a apresentação de declarações de apoio em duplicado.

Segurança ao nível da aplicação

- 2.7. O sistema encontra-se devidamente protegido contra vulnerabilidades e ataques *exploit* conhecidos. Para esse efeito, satisfaz, entre outros, os seguintes requisitos:
 - 2.7.1. O sistema impede falhas de injeção como interrogações SQL (*Structured Query Language*), LDAP (*Lightweight Directory Access Protocol*) ou XPath (*XML Path Language*), comandos do sistema operativo (SO) ou argumentos de um programa. Para o efeito, exige-se, no mínimo, que:
 - a) Todos os dados introduzidos pelos utilizadores sejam validados;
 - b) A validação seja efectuada, pelo menos, pela lógica do servidor;
 - c) A utilização de quaisquer interpretadores separe claramente os dados não fiáveis do comando ou da consulta. Para chamadas SQL, isto implica utilizar variáveis de substituição (*bind variables*) em todas as declarações elaboradas e procedimentos armazenados, e evitar interrogações dinâmicas.
 - 2.7.2. O sistema impede o XSS (*Cross-Site Scripting*). Para o efeito, exige-se, no mínimo, que:
 - a) Todos os dados fornecidos pelos utilizadores e reenviados ao navegador (*browser*) sejam verificados quanto à sua segurança (através de validação dos dados introduzidos);
 - b) Todos os dados introduzidos pelos utilizadores sejam submetidos a uma sequência de escape adequada antes de serem incluídos na página de saída;
 - c) A codificação adequada dos dados de saída assegure que esses dados introduzidos sejam sempre tratados como texto no navegador. Não são utilizados conteúdos activos.
 - 2.7.3. O sistema assegura uma autenticação forte e a gestão das sessões, o que exige, no mínimo, que:
 - a) As credenciais sejam sempre protegidas quando armazenadas com recurso a técnicas de controlo da integridade dos dados (*hashing*) ou de cifragem dos dados. O risco de alguém se autenticar utilizando a técnica *pass-the-hash* é assim mitigado;
 - b) As credenciais não possam ser adivinhadas nem alteradas através de funções de gestão da conta pouco sólidas (por exemplo, criação de conta, alteração da senha, recuperação da senha, identificadores de sessão frágeis);
 - c) Os identificadores de sessão e os dados da sessão não se encontrem expostos no localizador uniforme de recursos (URL);
 - d) Os identificadores de sessão não sejam vulneráveis a ataques de fixação de sessão;
 - e) Os identificadores de sessão tenham um tempo-limite de operação, o que assegura que o utilizador sai do sistema;
 - f) Não haja lugar a rotação dos identificadores de sessão após o início bem-sucedido da sessão;
 - g) As senhas, os identificadores de sessão e outras credenciais sejam enviados apenas através do protocolo TLS (*Transport Layer Security*);

- h) As componentes de administração do sistema se encontrem devidamente protegidas. Se estiverem protegidas por um sistema de autenticação de factor único, a senha é composta por um mínimo de 10 caracteres, incluindo, no mínimo, uma letra, um algarismo e um carácter especial. Em alternativa, pode ser utilizada uma solução de autenticação de dois factores. Nos casos em que é utilizada a autenticação de factor único, esta inclui um mecanismo de verificação em duas fases para o acesso à parte de administração do sistema através da internet, no qual o factor único é reforçado por outro meio de autenticação, como uma senha ou um código usados apenas uma vez via SMS, ou uma sequência aleatória de caracteres cifrados de forma assimétrica a decifrar utilizando a chave privada dos organizadores/administradores, desconhecida do sistema.
- 2.7.4. O sistema não contém referências directas a objectos inseguras. Para o efeito, exige-se, no mínimo, que:
- No caso de referências directas a recursos restritos, a aplicação verifique que o utilizador está autorizado a aceder concretamente ao recurso pretendido;
 - Tratando-se de uma referência indirecta, a correspondência com a referência directa se cinja a valores autorizados para o utilizador em questão.
- 2.7.5. O sistema impede solicitações forçadas intersítios.
- 2.7.6. O sistema possui uma configuração de segurança adequada, o que exige, no mínimo, que:
- Todos os elementos de *software* estejam actualizados, nomeadamente o SO, o servidor *web* e o servidor de aplicações, o sistema de gestão de bases de dados (DBMS), as aplicações, e todas as bibliotecas de códigos;
 - Os serviços desnecessários do SO bem como do servidor *web* e do servidor de aplicações sejam desactivados, retirados ou não sejam instalados;
 - As senhas da conta por defeito sejam alteradas ou desactivadas;
 - O sistema de correcção de erros criado seja de molde a impedir fugas de rastreamentos em pilha (*stack traces*) e outras mensagens de erro demasiado informativas;
 - Os parâmetros de segurança nos quadros e bibliotecas de desenvolvimento estejam configurados de acordo com as melhores práticas, como as orientações do projecto OWASP.
- 2.7.7. Para a cifragem dos dados, o sistema prevê o seguinte:
- Os dados pessoais em formato electrónico são cifrados quando armazenados ou transmitidos às autoridades competentes dos Estados-Membros nos termos do artigo 8.º, n.º 1, do Regulamento (UE) n.º 211/2011, sendo as chaves geridas e guardadas separadamente;
 - São utilizados algoritmos correntes fortes e chaves fortes, conformes às normas internacionais. A gestão de chaves é parte integrante do sistema;
 - A integridade das senhas é controlada com técnicas *hash* que utilizam um algoritmo corrente forte e com técnicas *salt* adequadas;
 - Todas as chaves e senhas estão protegidas contra qualquer acesso não autorizado.
- 2.7.8. O sistema limita o acesso ao URL com base nos níveis e autorizações de acesso do utilizador. Para o efeito, exige-se, no mínimo, que:
- Se forem utilizados mecanismos de segurança externos para fins de autenticação e verificação das autorizações de acesso às páginas, os mesmos devem estar devidamente configurados para cada página;
 - Se for utilizada protecção ao nível dos códigos, a mesma deve existir para cada página pretendida.
- 2.7.9. O sistema utiliza o protocolo TLS (*Transport Layer Security*) de modo a garantir uma protecção suficiente. Para o efeito, estão criadas todas as medidas que se seguem ou outras com uma eficácia, no mínimo, equivalente:
- O sistema exige a versão mais actualizada do protocolo HTTPS (*Hypertext Transfer Protocol Secure*) para aceder a quaisquer recursos sensíveis utilizando certificados que sejam válidos, não caducados, não revogados e compatíveis com todos os domínios utilizados pelo sítio;
 - O sistema apõe a indicação «seguro» em todos os *cookies* sensíveis;
 - O servidor configura o fornecedor do TLS de modo que este apenas aceite algoritmos de cifragem de dados conformes com as melhores práticas. Os utilizadores são informados de que devem activar a funcionalidade TLS no seu navegador.
- 2.7.10. O sistema impede reencaminhamentos e reenvios não validados.

Segurança das bases de dados e integridade dos dados

- 2.8. Sempre que os sistemas de recolha por via electrónica utilizados para diferentes iniciativas de cidadania partilhem *hardware* e recursos do sistema operativo, não partilharão quaisquer dados, nomeadamente credenciais de acesso e de cifragem. Por outro lado, esta situação reflecte-se na avaliação de riscos e nas contramedidas aplicadas.
- 2.9. O risco de alguém se autenticar na base de dados utilizando a técnica *pass-the-hash* é mitigado.
- 2.10. O acesso aos dados fornecidos pelos subscritores é disponibilizado apenas ao administrador/organizador da base de dados.
- 2.11. As credenciais administrativas, os dados pessoais recolhidos junto dos subscritores e o respectivo *backup* são securizados por meio de algoritmos de criptografia seguros, de acordo com o ponto 2.7.7, alínea b). No entanto, outros dados, como os que identificam o Estado-Membro em que a declaração de apoio será contada, a data de apresentação da declaração de apoio e a língua utilizada pelo subscritor no preenchimento da declaração de apoio, podem ser armazenados sem cifragem no sistema.
- 2.12. Os subscritores apenas têm acesso aos dados introduzidos na sessão em que preenchem o formulário da declaração de apoio. Uma vez enviado o formulário, a sessão é encerrada e os dados introduzidos deixam de estar acessíveis.
- 2.13. Os dados pessoais dos subscritores, incluindo o respectivo *backup*, estão disponíveis no sistema apenas em formato cifrado. Para efeitos de consulta dos dados ou certificação pelas autoridades nacionais nos termos do artigo 8.º do Regulamento (UE) n.º 211/2011, os organizadores podem exportar os dados cifrados de acordo com o ponto 2.7.7, alínea a).
- 2.14. A persistência dos dados introduzidos no formulário de declaração de apoio é atómica. Quer isto dizer que, assim que o utilizador introduz todos os dados necessários no formulário de declaração de apoio e valida a sua decisão de apoiar a iniciativa, o sistema ou regista com êxito todos os dados do formulário na base de dados ou, em caso de erro, aborta a operação e não guarda quaisquer dados. O sistema informa o utilizador sobre o êxito ou o fracasso do seu pedido.
- 2.15. O sistema DBMS utilizado está actualizado e é continuamente corrigido (*patched*), à medida que são descobertos novos ataques *exploit*.
- 2.16. Estão criados todos os registos da actividade do sistema. O sistema assegura que os registos de auditoria das excepções e de outros eventos relevantes para a segurança, abaixo enumerados, podem ser produzidos e mantidos até os dados serem destruídos, nos termos do artigo 12.º, n.º 3 ou 5, do Regulamento (UE) n.º 211/2011. Os registos são adequadamente protegidos, através, por exemplo, de armazenamento em suportes cifrados. Os organizadores/administradores verificam periodicamente os registos para detecção de qualquer actividade suspeita. O conteúdo dos registos é, no mínimo, o seguinte:
- Datas e horas do início (*log-on*) e do fim (*log-off*) das sessões pelos organizadores/administradores;
 - Backups* efectuados;
 - Todas as alterações e actualizações ao nível do administrador da base de dados.

Segurança das infra-estruturas – localização física, infra-estrutura de rede e ambiente do servidor

- 2.17. *Segurança física*
- Qualquer que seja o tipo de alojamento utilizado, a máquina que aloja a aplicação está devidamente protegida, o que implica:
- Controlo do acesso à zona de alojamento e registo de actividades;
 - Protecção física dos dados de *backup* contra roubo ou extravio accidental;
 - Que o servidor em que a aplicação se encontra hospedada esteja instalado num bastidor securizado.
- 2.18. *Segurança da rede*
- 2.18.1. O sistema está alojado num servidor com ligação directa à internet instalado numa zona desmilitarizada (DMZ) e protegido por uma *firewall*.
- 2.18.2. Quando são publicadas actualizações e correcções relevantes do produto *firewall*, tais actualizações e correcções são instaladas de forma expedita.
- 2.18.3. Todo o tráfego de entrada e de saída no servidor (destinado ao sistema de recolha por via electrónica) é inspeccionado à luz das regras de *firewall* e registado. As regras de *firewall* rejeitam o tráfego que não é necessário à utilização e à administração seguras do sistema.
- 2.18.4. O sistema de recolha por via electrónica deve ser alojado num segmento da rede de produção devidamente protegido, separado dos segmentos utilizados para alojar sistemas que não são de produção, como ambientes de desenvolvimento ou de ensaio.

2.18.5. Estão criadas medidas de segurança da rede local (LAN), designadamente as seguintes:

- a) Lista de acesso à camada 2 (L2)/segurança do comutador de portas;
- b) As portas do comutador não utilizadas são desactivadas;
- c) A DMZ encontra-se numa rede local virtual (VLAN)/LAN própria;
- d) Não estão activadas interligações (*trunking*) L2 em portas desnecessárias.

2.19. *Segurança do SO, do servidor web e do servidor de aplicações*

2.19.1. Existe uma configuração de segurança adequada, que inclui os elementos enumerados no ponto 2.7.6.

2.19.2. As aplicações operam com o menor conjunto de privilégios de que necessitam para operar.

2.19.3. O acesso dos administradores à interface de gestão do sistema de recolha por via electrónica tem um tempo-limite curto (15 minutos, no máximo).

2.19.4. Quando são publicadas actualizações e correcções relevantes do SO, dos motores de execução das aplicações, das aplicações executadas nos servidores ou das protecções anti-*malware*, tais actualizações e correcções são instaladas de forma expedita.

2.19.5. O risco de alguém se autenticar no sistema utilizando a técnica *pass-the-hash* é mitigado.

2.20. *Segurança do cliente do organizador*

Com vista à segurança extremo-a-extremo, os organizadores tomam as medidas necessárias para securizar a aplicação-cliente ou o dispositivo-cliente que utilizam para gerir e aceder ao sistema de recolha por via electrónica, designadamente as seguintes:

2.20.1. Os utilizadores executam tarefas que não sejam de manutenção (por exemplo, de burótica) com o menor conjunto de privilégios de que necessitam para essa execução.

2.20.2. Quando são publicadas actualizações e correcções relevantes do SO, de quaisquer aplicações instaladas ou das protecções anti-*malware*, tais actualizações e correcções são instaladas de forma expedita.

3. ESPECIFICAÇÕES TÉCNICAS COM VISTA À APLICAÇÃO DO ARTIGO 6.º, N.º 4, ALÍNEA c) DO REGULAMENTO (UE) N.º 211/2011

3.1. O sistema prevê a possibilidade de extrair, para cada Estado-Membro, um relatório com a indicação da iniciativa e dos dados pessoais dos subscritores, a verificar pela autoridade competente do Estado-Membro em causa.

3.2. A exportação das declarações de apoio dos subscritores é possível no formato do anexo III do Regulamento (UE) n.º 211/2011. O sistema prevê, além disso, a possibilidade de exportar as declarações de apoio num formato interoperável, como o XML (*eXtensible Markup Language*).

3.3. As declarações de apoio exportadas são assinaladas como sendo de *distribuição limitada* ao Estado-Membro em causa, e rotuladas como *dados pessoais*.

3.4. A transmissão electrónica de dados exportados para os Estados-Membros é securizada contra intercepções não autorizadas através do recurso a criptografia adequada extremo-a-extremo.
