II

(Atos não legislativos)

REGULAMENTOS

REGULAMENTO DE EXECUÇÃO (UE) 2019/1799 DA COMISSÃO

de 22 de outubro de 2019

que estabelece as especificações técnicas a que devem obedecer os sistemas de recolha em linha, nos termos do Regulamento (UE) 2019/788 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) 2019/788 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, sobre a iniciativa de cidadania europeia ([1]), nomeadamente o artigo 11.º, n.º 5,

Considerando o seguinte:

(1) O Regulamento (UE) 2019/788 revê as regras relativas à iniciativa de cidadania europeia, revogando o Regulamento (UE) n.º 211/2011 do Parlamento Europeu e do Conselho ([2]).

(2) O Regulamento (UE) 2019/788 prevê que, para efetuar a recolha em linha de declarações de apoio a iniciativas de cidadania registadas, os organizadores utilizem o sistema central de recolha em linha criado e operado pela Comissão. No entanto, para facilitar a transição, no que se refere às iniciativas registadas ao abrigo do Regulamento (UE) 2019/788 até ao final de 2022, os organizadores podem optar por utilizar o seu próprio sistema de recolha em linha.

(3) Nos termos do Regulamento (UE) 2019/788, qualquer sistema utilizado para a recolha em linha de declarações de apoio deve ter características técnicas e de segurança adequadas que garantam que os dados são recolhidos, conservados e transmitidos de forma segura durante todo o processo de recolha. Para o efeito, a Comissão deve definir, juntamente com os Estados-Membros, as especificações técnicas necessárias para implementar esses requisitos relativamente a cada sistema de recolha em linha.

(4) As regras estabelecidas no presente regulamento substituem as estabelecidas no Regulamento de Execução (UE) n.º 1179/2011 da Comissão ([3]), que, por conseguinte, se tornam obsoletas.

(5) As medidas técnicas e organizativas que devem ser aplicadas devem ter por objetivo evitar, tanto no momento da conceção do sistema como durante todo o período de recolha, qualquer tratamento não autorizado de dados pessoais, protegendo-os de uma destruição acidental ou ilícita ou de uma perda acidental ou alteração ou, ainda, da divulgação ou acesso não autorizados.

([1]) JO L 130 de 17.5.2019, p. 55.
([2]) Regulamento (UE) n.º 211/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, sobre a iniciativa de cidadania (JO L 65 de 11.3.2011, p. 1).
([3]) 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 eletrónica, nos termos do Regulamento (UE) n.º 211/2011 do Parlamento Europeu e do Conselho sobre a iniciativa de cidadania (JO L 301 de 18.11.2011, p. 3).

(6) Para o efeito, os organizadores devem observar procedimentos adequados de gestão de riscos, que permitam identificar os riscos a que estão sujeitos os seus sistemas e conceber contramedidas adequadas e proporcionais para reduzir os riscos em causa para níveis aceitáveis. Os organizadores devem documentar devidamente os riscos identificados em matéria de segurança e proteção de dados e as medidas tomadas para os combater, tendo em conta as regras e os requisitos de segurança aplicados pela autoridade de certificação. As regras e os requisitos de segurança devem respeitar o disposto no Regulamento (UE) 2019/788, devendo ser disponibilizados pela autoridade de certificação, a pedido.

(7) A aplicação das especificações técnicas estabelecidas no presente regulamento não prejudica a obrigação de os organizadores cumprirem os requisitos em matéria de proteção de dados decorrentes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([4]), incluindo a eventual necessidade de uma avaliação de impacto relativa à proteção de dados.

(8) O representante de um grupo de organizadores ou, se for caso disso, uma entidade jurídica, tal como referida no artigo 5.º, n.º 7, do regulamento em questão, é considerado responsável pelo tratamento de dados, nos termos do Regulamento (UE) 2016/679, no que diz respeito ao tratamento dos dados pessoais no âmbito de um sistema de recolha em linha.

(9) Os organizadores que introduzam alterações no seu próprio sistema de recolha em linha depois de este ter sido devidamente certificado devem notificar sem demora injustificada a autoridade de certificação competente, caso essa alteração seja suscetível de afetar a avaliação em que se baseia a certificação. Antes de o fazer, os organizadores podem solicitar o parecer da autoridade de certificação sobre se a alteração em causa pode ter tal impacto e se, por conseguinte, deve ser notificada.

(10) A Autoridade Europeia para a Proteção de Dados, consultada em conformidade com o artigo 42.º do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([5]), apresentou as suas observações em 16 de setembro de 2019. Foi também consultada a Agência Europeia para a Segurança das Redes, que apresentou as suas observações em 18 de julho de 2019.

(11) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité criado pelo artigo 22.º do Regulamento (UE) 2019/788,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

As especificações técnicas referidas no artigo 11.º, n.º 5, do Regulamento (UE) 2019/788 são estabelecidas no anexo do presente regulamento.

Artigo 2.º

1. Os organizadores devem assegurar que o seu sistema de recolha em linha cumpre as especificações técnicas estabelecidas no anexo durante todo o período de recolha.

2. Os organizadores devem notificar sem demora injustificada a autoridade competente do Estado-Membro a que se refere o artigo 11.º, n.º 3, do Regulamento (UE) 2019/788 de quaisquer alterações introduzidas no sistema ou nas medidas organizativas de apoio após o sistema ter sido certificado por essa autoridade, sempre que essas alterações possam afetar a avaliação em que se baseia a certificação. Antes de o fazer, os organizadores podem solicitar o parecer da autoridade de certificação para determinar se a alteração em causa pode ter tal impacto.

([4]) 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).

([5]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

Artigo 3.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 aplicável a partir de 1 de janeiro de 2020.

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

Feito em Bruxelas, em 22 de outubro de 2019.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

ANEXO

1. **ESPECIFICAÇÕES TÉCNICAS PARA A APLICAÇÃO DO ARTIGO 11.º, N.º 4, ALÍNEA A), DO REGULAMENTO (UE) 2019/788**

O sistema deve incluir medidas técnicas que garantam que apenas as pessoas singulares podem apresentar declarações de apoio. As medidas técnicas não podem exigir que sejam recolhidos e armazenados mais dados do que os enumerados no anexo III do Regulamento (UE) 2019/788.

2. **ESPECIFICAÇÕES TÉCNICAS PARA A APLICAÇÃO DO ARTIGO 11.º, N.º 4, ALÍNEA B), DO REGULAMENTO (UE) 2019/788**

Os organizadores devem adotar medidas técnicas e organizativas adequadas e eficazes para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações, a fim de assegurar que as informações prestadas sobre a iniciativa no sistema de recolha em linha e publicadas em linha correspondem às informações sobre a iniciativa publicadas no registo referido no artigo 6.º, n.º 5, do Regulamento (UE) 2019/788.

Os organizadores devem certificar-se de que:

a) as informações facultadas sobre a iniciativa no sistema de recolha em linha correspondem às informações publicadas no registo;

b) o sistema apresenta as informações sobre a iniciativa publicadas no registo antes de o cidadão apresentar a sua declaração de apoio;

c) foram tomadas as medidas de segurança para assegurar que os campos de introdução de dados das declarações de apoio são apresentados juntamente com as informações sobre a iniciativa, a fim de evitar o risco de as declarações de apoio serem associadas a uma iniciativa diferente daquela a que se destinavam inicialmente mediante uma deturpação da iniciativa;

d) o sistema garante que, após a apresentação, os dados das declarações de apoio são guardados juntamente com as informações sobre a iniciativa;

e) existem medidas de segurança para impedir a introdução de alterações não autorizadas nas informações facultadas sobre a iniciativa no sistema de recolha em linha.

3. **ESPECIFICAÇÕES TÉCNICAS PARA A APLICAÇÃO DO ARTIGO 11.º, N.º 4, ALÍNEA C), DO REGULAMENTO (UE) 2019/788**

O sistema deve assegurar que as declarações de apoio são apresentadas de acordo com os campos de dados constantes do anexo III do Regulamento (UE) 2019/788.

O sistema deve assegurar que a declaração de apoio só pode ser apresentada após a pessoa ter confirmado que leu a declaração de confidencialidade que consta do anexo III do Regulamento (UE) 2019/788.

4. **ESPECIFICAÇÕES TÉCNICAS PARA A APLICAÇÃO DO ARTIGO 11.º, N.º 4, ALÍNEA D), DO REGULAMENTO (UE) 2019/788**

4.1. **Governação**

4.1.1. O grupo de organizadores deve nomear um responsável pela segurança, que será responsável pela segurança do sistema e pela transmissão segura das declarações de apoio recolhidas à autoridade competente do Estado-Membro responsável. O responsável pela segurança deve supervisionar os processos de garantia das informações e as medidas de segurança técnica e organizativa, que visam garantir a segurança da recolha, armazenamento e transmissão dos dados facultados pelos subscritores.

4.1.2. Os organizadores podem solicitar à autoridade nacional competente referida no artigo 11.º, n.º 3, do Regulamento (UE) 2019/788 que faculte informações sobre as regras e os requisitos de segurança aplicáveis à certificação de cada sistema de recolha em linha. Regra geral, a autoridade competente deve comunicar essas regras e os requisitos de segurança no prazo de um mês após a receção do pedido. Essas regras e requisitos devem ser conformes com as regras de segurança nacionais ou internacionais aplicáveis.

4.1.3. As regras e os requisitos de segurança aplicáveis à certificação do sistema devem visar especificamente os riscos enumerados no ponto 4.2 e ter em conta as especificações constantes do ponto 4.3.

4.2. **Garantia da informação**

4.2.1. Os organizadores devem utilizar processos de gestão de riscos para identificar os riscos associados à utilização dos respetivos sistemas, nomeadamente os riscos para os direitos e liberdades dos subscritores, e para determinar as medidas mais adequadas e proporcionais para prevenir e atenuar o impacto de incidentes que afetem a segurança da rede e dos sistemas de informação utilizados nas respetivas operações.

O processo de gestão de riscos deve centrar-se, em especial, nos riscos relacionados com a confidencialidade e a integridade das informações no sistema. Estes riscos podem resultar das seguintes ameaças:

a) erros do utilizador;

b) erros do administrador do sistema/de segurança;

c) erros de configuração;

d) infeção por *software* mal-intencionado;

e) alteração acidental de informações;

f) fugas ou divulgação de informações;

g) vulnerabilidades do *software*;

h) acesso não autorizado;

i) interceção ou espionagem do tráfego;

j) riscos relativos à proteção de dados.

4.2.2. Os organizadores devem fornecer documentação comprovativa de que:

a) foi efetuada uma avaliação dos riscos do sistema;

b) foram adotadas medidas adequadas para prevenir e atenuar o impacto de incidentes que afetem a segurança do sistema;

c) foram identificados os riscos residuais;

d) foram adotadas as medidas em causa e verificada a sua aplicação;

e) foram criados os meios organizacionais necessários para receber informações sobre novas ameaças e melhorias em matéria de segurança;

f) foram cumpridos, ao longo de todo o processo de recolha, os requisitos de certificação estabelecidos no artigo 11.º, n.º 4, do Regulamento (UE) 2019/788, incluindo a implantação dos processos necessários para o efeito.

4.2.3. As medidas destinadas a prevenir e atenuar o impacto de incidentes que afetem a segurança dos sistemas devem abarcar os seguintes domínios:

a) segurança dos recursos humanos;

b) controlo do acesso;

c) controlos criptográficos;

d) segurança física e ambiental;

e) segurança das operações;

f) segurança das comunicações;

g) aquisição, desenvolvimento e manutenção dos sistemas;

h) gestão dos incidentes de segurança da informação;

i) conformidade.

A aplicação destas medidas de segurança pode cingir-se às partes da organização mais relevantes para o sistema de recolha em linha. Por exemplo, a segurança dos recursos humanos pode ser limitada aos elementos do pessoal com acesso físico ou lógico ao sistema de recolha em linha e a segurança física e ambiental pode ser limitada ao(s) edifício (s) onde está alojado o sistema.

4.2.4. Quando recorrera a um processador para o desenvolvimento ou implantação dos sistemas de recolha em linha ou de partes dos mesmos, os organizadores devem apresentar documentação que permita à autoridade de certificação verificar se foram criados os controlos de segurança necessários.

4.3. **Cifragem de dados**

O sistema deve prever a cifragem de dados nos seguintes casos:

a) Os dados pessoais em formato eletrónico devem ser cifrados quando armazenados ou transmitidos às autoridades competentes dos Estados-Membros, em conformidade com o disposto no Regulamento (UE) 2019/788, sendo as chaves geridas e guardadas separadamente;

b) Devem ser utilizados algoritmos correntes adequados e chaves adequadas em conformidade com as regras internacionais (como a norma ETSI), devendo a gestão de chaves fazer parte integrante do sistema;

c) todas as chaves e senhas devem estar protegidas contra o eventual acesso não autorizado.