II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) 2019/1799 DE LA COMISIÓN

de 22 de octubre de 2019

por el que se establecen especificaciones técnicas para sistemas individuales de recogida en línea, de conformidad con el Reglamento (UE) 2019/788 del Parlamento Europeo y del Consejo sobre la iniciativa ciudadana europea

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/788 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la iniciativa ciudadana europea ([1]), y en particular su artículo 11, apartado 5,

Considerando lo siguiente:

(1) El Reglamento (UE) 2019/788 establece normas revisadas sobre la iniciativa ciudadana europea y deroga el Reglamento (UE) n.º 211/2011 del Parlamento Europeo y del Consejo ([2]).

(2) El Reglamento (UE) 2019/788 establece que, para la recogida en línea de declaraciones de apoyo a las iniciativas ciudadanas registradas, los organizadores deben utilizar el sistema central de recogida en línea creado y gestionado por la Comisión. Sin embargo, para facilitar la transición, en el caso de las iniciativas registradas con arreglo al Reglamento (UE) 2019/788 antes del final de 2022, los organizadores pueden optar por utilizar su propio sistema de recogida en línea.

(3) En virtud del Reglamento (UE) 2019/788, los sistemas individuales que se utilicen para la recogida en línea de declaraciones de apoyo deben tener características técnicas y de seguridad adecuadas para garantizar que los datos se recojan, almacenen y transfieran de manera segura durante el procedimiento de recogida. La Comisión debe definir, junto con los Estados miembros, las especificaciones técnicas que deben reunir los sistemas individuales de recogida en línea para cumplir los requisitos del Reglamento.

(4) Las normas establecidas en el presente Reglamento sustituyen a las del Reglamento de Ejecución (UE) n.º 1179/2011 de la Comisión ([3]), que, por lo tanto, quedarán obsoletas.

(5) Las medidas técnicas y organizativas que deban aplicarse deben tener por objeto evitar, tanto en el momento de la concepción del sistema como durante todo el período de recogida, cualquier tratamiento no autorizado de datos personales y protegerlos contra la destrucción accidental o ilícita, la pérdida accidental, la alteración o la difusión o el acceso no autorizados.

([1]) DO L 130 de 17.5.2019, p. 55.
([2]) Reglamento (UE) n.º 211/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, sobre la iniciativa ciudadana (DO L 65 de 11.3.2011, p. 1).
([3]) Reglamento de Ejecución (UE) n.º 1179/2011 de la Comisión, de 17 de noviembre de 2011, por el que se establecen especificaciones técnicas para sistemas de recogida en línea, de conformidad con el Reglamento (UE) n.º 211/2011 del Parlamento Europeo y del Consejo sobre la iniciativa ciudadana (DO L 301 de 18.11.2011, p. 3).

(6) A tal fin, los organizadores deben aplicar procedimientos adecuados de gestión de riesgos para detectar los riesgos para sus sistemas y determinar contramedidas apropiadas y proporcionales que reduzcan dichos riesgos a niveles aceptables. Los organizadores documentarán adecuadamente los riesgos detectados en materia de seguridad y protección de datos y las medidas adoptadas para contrarrestarlos, teniendo en cuenta las normas y requisitos de seguridad aplicados por la autoridad de certificación. Las normas y requisitos de seguridad deben estar en consonancia con el Reglamento (UE) 2019/788 y deben facilitados por la autoridad de certificación, previa solicitud.

(7) La aplicación de las especificaciones técnicas establecidas en el presente Reglamento debe entenderse sin perjuicio de la obligación de los organizadores de cumplir los requisitos de protección de datos que se derivan del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([4]), incluida la posible necesidad de realizar una evaluación de impacto relativa a la protección de datos.

(8) El representante de un grupo de organizadores o, en su caso, una persona jurídica, como se contempla en el artículo 5, apartado 7, de dicho Reglamento, se considerará responsable del tratamiento de datos en el sentido del Reglamento (UE) 2016/679 en relación con el tratamiento de datos personales en un sistema individual de recogida en línea.

(9) Los organizadores que introduzcan cambios en su sistema individual de recogida en línea después de que el sistema haya sido certificado deben notificar sin dilación indebida a la autoridad de certificación pertinente si el cambio puede afectar a la evaluación en que se basa la certificación. Antes de hacerlo, los organizadores pueden solicitar el dictamen de la autoridad de certificación sobre si el cambio puede tener tal impacto.

(10) El Supervisor Europeo de Protección de Datos, que fue consultado de conformidad con el artículo 42 del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([5]), presentó sus observaciones el 16 de septiembre de 2019. Se consultó a la Agencia Europea de Seguridad de las Redes y de la Información, que presentó sus observaciones el 18 de julio de 2019.

(11) Las medidas contempladas en el presente Reglamento se ajustan al dictamen del Comité creado en virtud del artículo 22 del Reglamento (UE) 2019/788.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Se fijan en el anexo del presente Reglamento las especificaciones técnicas a que se hace referencia en el artículo 11, apartado 5, del Reglamento (UE) 2019/788.

Artículo 2

1. Los organizadores se asegurarán de que su sistema individual de recogida en línea se ajuste a las especificaciones técnicas establecidas en el anexo durante todo el período de recogida.

2. Los organizadores notificarán, sin dilación indebida, a la autoridad competente del Estado miembro mencionada en el artículo 11, apartado 3, del Reglamento (UE) 2019/788 los cambios introducidos en el sistema o en las medidas organizativas de apoyo después de que el sistema haya sido certificado por dicha autoridad, cuando dichos cambios puedan afectar a la evaluación en que se basa la certificación. Antes de hacerlo, los organizadores podrán solicitar el dictamen de la autoridad competente sobre si el cambio puede tener tal impacto.

([4]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

([5]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

Artículo 3

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del 1 de enero de 2020.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 22 de octubre de 2019.

Por la Comisión
El Presidente
Jean-Claude JUNCKER

ANEXO

1. **ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 11, APARTADO 4, LETRA A), DEL REGLAMENTO (UE) 2019/788**

El sistema incluirá medidas técnicas para garantizar que solo las personas físicas puedan presentar declaraciones de apoyo. Las medidas técnicas no exigirán que se recojan y almacenen más datos personales que los que figuran en el anexo III del Reglamento (UE) 2019/788.

2. **ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 11, APARTADO 4, LETRA B), DEL REGLAMENTO (UE) 2019/788**

Los organizadores adoptarán medidas técnicas y organizativas adecuadas y eficaces para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que utilicen en sus operaciones, a fin de garantizar que la información facilitada sobre la iniciativa en el sistema de recogida en línea y publicada en línea corresponda a la información publicada sobre la iniciativa en el registro a que se refiere el artículo 6, apartado 5, del Reglamento (UE) 2019/788.

Los organizadores se asegurarán de que:

a) la información facilitada sobre la iniciativa en el sistema de recogida en línea corresponda a la información publicada en el registro;

b) el sistema presente la información sobre la iniciativa publicada en el registro antes de que el ciudadano presente la declaración de apoyo;

c) se pongan en marcha medidas de seguridad que garanticen que las casillas para la introducción de datos en las declaraciones de apoyo se presenten junto con la información sobre la iniciativa, con el fin de evitar el riesgo de que las declaraciones de apoyo se presenten para una iniciativa diferente por una tergiversación de la iniciativa;

d) el sistema garantice que, después de la presentación, los datos de las declaraciones de apoyo se guarden junto con la información sobre la iniciativa;

e) existan medidas de seguridad para evitar que puedan introducirse cambios no autorizados en la información facilitada sobre la iniciativa en el sistema de recogida en línea.

3. **ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 11, APARTADO 4, LETRA C), DEL REGLAMENTO (UE) 2019/788**

El sistema garantizará que las declaraciones de apoyo se presenten de conformidad con las casillas de datos del anexo III del Reglamento (UE) 2019/788.

El sistema garantizará que una persona solo pueda presentar una declaración de apoyo tras haber confirmado que ha leído la declaración de privacidad del anexo III del Reglamento (UE) 2019/788.

4. **ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 11, APARTADO 4, LETRA D), DEL REGLAMENTO (UE) 2019/788**

4.1. **Gobernanza**

4.1.1. El grupo de organizadores nombrará a un responsable de seguridad que se encargará de la seguridad del sistema y de la transmisión segura de las declaraciones de apoyo recogidas a la autoridad competente del Estado miembro competente. El responsable de seguridad supervisará los procesos de aseguramiento de la información y las medidas de seguridad técnicas y organizativas necesarias para garantizar la recogida, el almacenamiento y la transmisión seguros de los datos facilitados por los firmantes.

4.1.2. Los organizadores podrán solicitar a la autoridad nacional competente mencionada en el artículo 11, apartado 3, del Reglamento (UE) 2019/788 que proporcione información sobre las normas y requisitos de seguridad aplicables a la certificación de los sistemas individuales de recogida en línea. La autoridad competente proporcionará la información sobre las normas y requisitos de seguridad, por regla general, en el plazo de un mes tras la recepción de la solicitud. Las normas y requisitos de seguridad aplicables deberán estar en consonancia con las normas nacionales o internacionales de seguridad equivalentes vigentes.

4.1.3. Las normas y requisitos de seguridad para la certificación del sistema deberán tratar los riesgos definidos en la sección 4.2 y tener en cuenta las especificaciones de la sección 4.3.

4.2. **Aseguramiento de la información**

4.2.1. Los organizadores utilizarán procesos de gestión de riesgos para detectar los riesgos vinculados al uso de sus sistemas, incluidos los derechos y las libertades de los firmantes, y para determinar medidas apropiadas y proporcionadas para prevenir y mitigar el impacto de los incidentes que afecten a la seguridad de la red y de los sistemas de información que utilicen en sus operaciones.

El proceso de gestión de riesgos se centrará especialmente en los riesgos relacionados con la confidencialidad e integridad de la información en el sistema. Estos riesgos pueden ser el resultado de amenazas, como:

a) errores de los usuarios;

b) errores del sistema o de los administradores de seguridad;

c) errores de configuración;

d) infecciones por programas informáticos maliciosos;

e) alteraciones accidentales de la información;

f) divulgaciones o filtraciones de información;

g) vulnerabilidades de los programas informáticos;

h) accesos no autorizados;

i) interceptación o espionaje del tráfico, y

j) riesgos de la protección de datos.

4.2.2. Los organizadores presentarán documentación que demuestre que:

a) han evaluado los riesgos del sistema;

b) han establecido medidas apropiadas para prevenir y mitigar el impacto de los incidentes que afecten a la seguridad del sistema;

c) han detectado los riesgos residuales;

d) han aplicado las medidas y comprobado su resultado;

e) han dispuesto los medios organizativos para mantenerse informados sobre las nuevas amenazas y las mejoras de seguridad, y

f) cumplen durante todo el proceso de recogida los requisitos de certificación establecidos en el artículo 11, apartado 4, del Reglamento (UE) 2019/788, incluido la implantación de los procesos necesarios para ello.

4.2.3. Las medidas de prevención y mitigación del impacto de los incidentes que afecten a la seguridad de los sistemas abarcarán los siguientes ámbitos:

a) seguridad de los recursos humanos;

b) control de acceso;

c) controles criptográficos;

d) seguridad física y del entorno;

e) seguridad de las operaciones;

f) seguridad de las comunicaciones;

g) adquisición, desarrollo y mantenimiento de sistemas;

h) gestión de incidentes de seguridad de la información;

i) cumplimiento.

La aplicación de estas medidas de seguridad puede limitarse a las partes de la organización que intervienen en el sistema de recogida en línea. Por ejemplo, la seguridad de los recursos humanos puede limitarse al personal que tengan acceso físico o lógico al sistema de recogida en línea, y la seguridad física y del entorno puede limitarse al edificio o edificios que alojen el sistema.

4.2.4. Cuando los organizadores recurran a procesador para el desarrollo o implantación de los sistemas de recogida en línea o de partes de los mismos, los organizadores deberán facilitar documentación que permita a la autoridad de certificación comprobar que se han establecido los controles de seguridad necesarios.

4.3. **Cifrado de datos**

El sistema contemplará el cifrado de datos siguiente:

a) los datos personales en formato electrónico se cifrarán cuando se almacenen o transmitan a las autoridades competentes de los Estados miembros de conformidad con el Reglamento (UE) 2019/788; se gestionarán las claves por separado y se hará una copia de seguridad de cada una también por separado;

b) se utilizarán algoritmos estándar adecuados y claves adecuadas de acuerdo con las normas internacionales (como la norma ETSI); deberá haber una gestión de claves;

c) todas las claves y contraseñas estarán protegidas contra los accesos no autorizados.