

REGLAMENTOS INTERNOS Y DE PROCEDIMIENTO

DECISIÓN DEL CONSEJO DE ADMINISTRACIÓN DE LA AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD

de 21 de noviembre de 2019

relativa a las normas internas sobre las limitaciones de determinados derechos de los interesados en relación con el tratamiento de datos personales en el marco del funcionamiento de la ENISA

EL CONSEJO DE ADMINISTRACIÓN DE LA ENISA

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 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.º 45/2001 y la Decisión n.º 1247/2002/CE ⁽¹⁾, y, en particular, su artículo 25,

Visto el Reglamento (UE) n.º 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a la ENISA (la Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») ⁽²⁾, y en concreto su artículo 15, apartado 1,

Visto el dictamen del Supervisor Europeo de Protección de Datos (en lo sucesivo, el «SEPD»), de jueves, 17 de octubre de 2019, y la orientación del SEPD sobre el artículo 25 del Reglamento (UE) n.º 2018/1725 y las normas internas.

Considerando lo siguiente:

- (1) De conformidad con lo dispuesto en el artículo 25, apartado 1, del Reglamento (UE) n.º 2018/1725, las limitaciones a la aplicación de los artículos 14 a 22, 35 y 36, y también del artículo 4 de dicho Reglamento en la medida en que sus disposiciones se correspondan con los derechos y obligaciones que disponen los artículos 14 a 22, deben basarse en normas internas adoptadas por la ENISA cuando no se encuentren fundamentadas en actos jurídicos adoptados con arreglo a los Tratados.
- (2) Estas normas internas, incluidas sus disposiciones sobre la evaluación de la necesidad y la proporcionalidad de la limitación, no deben aplicarse cuando un acto jurídico adoptado con arreglo a los Tratados prevea una limitación de los derechos de los interesados.
- (3) Cuando la ENISA ejerza sus funciones en relación con los derechos de los interesados en virtud del Reglamento (UE) n.º 2018/1725, analizará si es aplicable alguna de las excepciones establecidas en dicho Reglamento.
- (4) En el marco de su funcionamiento administrativo, la ENISA puede realizar investigaciones administrativas, tramitar procedimientos disciplinarios, llevar a cabo actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF, tramitar casos de denuncia de irregularidades, tramitar procedimientos (formales e informales) en casos de acoso, tramitar quejas internas y externas, realizar auditorías internas, llevar a cabo evaluaciones de incidentes de ciberseguridad con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, emprender investigaciones a través del responsable de protección de datos en consonancia con lo dispuesto en el artículo 45, apartado 2, del Reglamento (UE) n.º 2018/1725 y llevar a cabo investigaciones internas sobre la seguridad (informática).

La ENISA trata diversas categorías de datos personales, incluidos los datos sólidos (datos «objetivos», como los datos de identificación, los datos de contacto, los datos profesionales, los datos administrativos, los datos recibidos de determinadas fuentes y los datos de las comunicaciones y el tráfico electrónicos) y los datos frágiles (datos «subjetivos» relacionados con el caso, como el razonamiento, los datos de comportamiento, las valoraciones, los datos de actuación y conducta, y los datos relacionados con el objeto del procedimiento o la actividad o presentados en relación con estos).

- (5) La ENISA, representada por su director ejecutivo, actúa como responsable del tratamiento de datos, con independencia de las posteriores delegaciones de esta función dentro de la propia ENISA al objeto de reflejar las diversas responsabilidades operativas por las distintas tareas de tratamiento de datos personales.

⁽¹⁾ DO L 295 de 21.11.2018, p. 39.

⁽²⁾ DO L 151 de 7.6.2019, p. 15.

- (6) Los datos personales se almacenan en un entorno electrónico o en papel de un modo seguro que impide el acceso ilícito a personas que no necesiten conocerlos y la transferencia ilícita a estas personas. Los datos personales tratados no se conservan durante un tiempo superior al necesario y al adecuado para los fines para los que se hubieran tratado, durante el período especificado en los avisos de protección de datos, las declaraciones de confidencialidad o los registros de la ENISA.
- (7) Estas normas internas deben aplicarse a todas las operaciones de tratamiento de datos llevadas a cabo por la ENISA en el ejercicio de sus indagaciones administrativas, procedimientos disciplinarios, actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF, procedimientos de denuncia de irregularidades, procedimientos (formales e informales) en casos de acoso, tramitación de quejas internas y externas, auditorías internas, evaluaciones de incidentes de ciberseguridad con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, investigaciones llevadas a cabo por el responsable de protección de datos en consonancia con lo dispuesto en el artículo 45, apartado 2, del Reglamento (UE) n.º 2018/1725 e investigaciones en materia de seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE).
- (8) Las normas internas deben aplicarse a las operaciones de tratamiento de datos llevadas a cabo antes del inicio de los procedimientos citados previamente, durante estos y durante el seguimiento de la actuación consecutiva a los resultados de dichos procedimientos. También se incluyen la asistencia y la cooperación prestadas por la ENISA a las autoridades nacionales y las organizaciones internacionales al margen de sus investigaciones administrativas.
- (9) En los casos en los que resulten aplicables estas normas internas, la ENISA debe justificar el carácter estrictamente necesario y proporcionado de las limitaciones en una sociedad democrática y respetar el contenido esencial de los derechos y las libertades fundamentales.
- (10) En este contexto, la ENISA debe respetar, en la medida de lo posible, los derechos fundamentales de los interesados durante los procedimientos anteriores, en particular, los correspondientes al derecho a la comunicación de información, el acceso y la rectificación, el derecho de supresión, la limitación del tratamiento, el derecho a la comunicación de una violación de la seguridad de los datos personales al interesado y la confidencialidad de las comunicaciones, de conformidad con el Reglamento (UE) n.º 2018/1725.
- (11) Sin embargo, la ENISA puede verse obligada a limitar la comunicación de información al interesado y otros derechos del interesado para proteger, en particular, sus propias investigaciones, las investigaciones y los procedimientos de otras autoridades públicas y los derechos de otras personas relacionadas con sus investigaciones o con los procedimientos de otro tipo que se lleven a cabo.
- (12) En consecuencia, la ENISA puede restringir la información a los efectos de proteger la investigación y los derechos y libertades fundamentales de otros interesados.
- (13) La ENISA debe controlar de manera periódica que se cumplan las condiciones que justifiquen la limitación y levantar la limitación en cuanto dejen de cumplirse.
- (14) El responsable del tratamiento debe realizar la notificación pertinente al responsable de protección de datos en el momento del aplazamiento y durante las revisiones.
- (15) Debido a la importancia de las normas internas para la protección de los derechos de los interesados, la Decisión debería entrar en vigor lo antes posible después de su publicación en el *Diario Oficial de la Unión Europea*.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Objeto y ámbito de aplicación

1. La siguiente Decisión establece las normas relativas a las condiciones en las que la ENISA, en el marco de sus procedimientos establecidos en el apartado 2, puede limitar el ejercicio de los derechos consagrados en los artículos 14 a 21, 35 y 36, y la aplicación del artículo 4, del Reglamento (UE) 2018/1725, de conformidad con el artículo 25 de este.
2. En el marco del funcionamiento administrativo de la ENISA, esta Decisión se aplica a las operaciones de tratamiento de datos personales llevadas a cabo por la ENISA a los efectos de hacer indagaciones administrativas, incoar procedimientos disciplinarios, llevar a cabo actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF, tramitar casos de denuncia de irregularidades (*whistleblowing*), procedimientos (formales e informales) para la prevención del acoso, así como reclamaciones internas y externas, realizar auditorías internas, evaluaciones de incidentes de ciberseguridad con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, investigaciones emprendidas por el responsable de protección de datos en consonancia con lo dispuesto en el artículo 45, apartado 2, del Reglamento (UE) n.º 2018/1725 e investigaciones en materia de seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE).

3. Las categorías de datos de que se trata son los datos sólidos (datos «objetivos», como los datos de identificación, los datos de contacto, los datos profesionales, los datos administrativos, los datos recibidos de determinadas fuentes y los datos de las comunicaciones y el tráfico electrónicos) y los datos frágiles (datos «subjetivos» relacionados con el caso, como el razonamiento, los datos de comportamiento, las valoraciones, los datos de actuación y conducta, y los datos relacionados con el objeto del procedimiento o la actividad o presentados en relación con estos).

4. Cuando la ENISA ejerza sus funciones en relación con los derechos de los interesados en virtud del Reglamento (UE) n.º 2018/1725, analizará si es aplicable alguna de las excepciones establecidas en dicho Reglamento.

5. Con arreglo a las condiciones previstas en la presente Decisión, las limitaciones pueden aplicarse a los siguientes derechos: la comunicación de información a los interesados, el derecho de acceso, la rectificación, la supresión, la limitación del tratamiento, la comunicación de una violación de la seguridad de los datos personales al interesado y la confidencialidad de las comunicaciones.

Artículo 2

Especificación del responsable del tratamiento y garantías

1. Las garantías establecidas para evitar las violaciones de la seguridad de los datos, las filtraciones o las divulgaciones no autorizadas son las siguientes:

- a) Los documentos en papel deberán conservarse en armarios protegidos a los que únicamente pueda acceder el personal autorizado.
- b) Todos los datos en formato electrónico deberán almacenarse en una aplicación informática segura que respete las normas de seguridad de la ENISA y en carpetas electrónicas específicas a las que únicamente pueda acceder el personal autorizado. Deberán concederse de manera individualizada los niveles de acceso adecuados.
- c) La base de datos estará protegida por contraseña en virtud de un sistema de autenticación única y conectada automáticamente al identificador y la contraseña del usuario. Queda terminantemente prohibido que los usuarios intercambien sus datos de identificación. Los registros electrónicos se almacenarán de forma segura para salvaguardar la confidencialidad y la privacidad de los datos que contengan.
- d) Todas las personas que dispongan de acceso a los datos quedarán sujetas a una obligación de confidencialidad.

2. El responsable de las operaciones de tratamiento será la ENISA, representada por su director ejecutivo, quien podrá delegar la función de responsable del tratamiento de datos. Se informará a los interesados de la identidad del responsable del tratamiento delegado por medio de avisos de protección de datos o de registros publicados en el sitio web o la intranet de la ENISA.

3. El período de conservación de los datos personales al que hace referencia el artículo 1, apartado 3, no superará el necesario ni el adecuado para los fines que justifiquen el tratamiento de los datos. En ningún caso deberá superar el período de conservación especificado en los avisos de protección de datos, las declaraciones de confidencialidad o los registros a los que se hace referencia en el artículo 5, apartado 1.

4. Cuando la ENISA estudie aplicar una limitación, deberá sopesarse el riesgo para los derechos y las libertades del interesado, en particular, con el riesgo para los derechos y las libertades de otros interesados y el riesgo de dejar sin efecto las investigaciones o los procedimientos emprendidos por la ENISA, por ejemplo, por la destrucción de pruebas. Los riesgos para los derechos y las libertades del interesado consisten principalmente, aunque no de manera exclusiva, en riesgos para la reputación y riesgos para el derecho a la defensa y a ser oído.

Artículo 3

Limitaciones

1. La ENISA solo adoptará limitaciones para salvaguardar:

- a) la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
- b) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular los objetivos de la política exterior y de seguridad común de la Unión o un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
- c) la seguridad interna de las instituciones y organismos de la Unión, incluida la de sus redes de comunicación electrónica;

- d) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
- e) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) y b);
- f) la protección del interesado o de los derechos y libertades de otros.

2. La evaluación de incidentes de ciberseguridad realizada por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881 («Reglamento sobre la Ciberseguridad») incluida en el apartado 1, letra b), del presente artículo.

3. Como aplicación concreta de los fines descritos en el apartado 1 anterior, la ENISA podrá introducir limitaciones en relación con los datos personales compartidos con los servicios de la Comisión u otras instituciones, órganos y organismos de la Unión, autoridades competentes de los Estados miembros o de terceros países u organizaciones internacionales, respectivamente en las siguientes circunstancias:

- a) cuando el ejercicio de esos derechos y el cumplimiento de esas obligaciones pueda ser limitado por los servicios de la Comisión o por otras instituciones, órganos y organismos de la Unión, sobre la base de los actos jurídicos contemplados en el artículo 25 del Reglamento (UE) n.º 2018/1725, o de conformidad con el capítulo IX de dicho Reglamento o con los actos fundacionales de otras instituciones, órganos y organismos de la Unión;
- b) cuando el ejercicio de esos derechos y el cumplimiento de esas obligaciones pueda verse limitado por las autoridades competentes de los Estados miembros sobre la base de los actos a que se refiere el artículo 23 del Reglamento (UE) n.º 2016/679 del Parlamento Europeo y del Consejo ⁽³⁾, o con arreglo a las medidas nacionales de transposición del artículo 13, apartado 3; del artículo 15, apartado 3; o del artículo 16, apartado 3, de la Directiva (UE) n.º 2016/680 del Parlamento Europeo y del Consejo ⁽⁴⁾;
- c) cuando el ejercicio de esos derechos y el cumplimiento de esas obligaciones pueda comprometer la cooperación de la ENISA con terceros países u organizaciones internacionales en el desempeño de sus funciones.

Antes de aplicar las limitaciones en las circunstancias mencionadas en el párrafo primero, letras a) y b), la ENISA consultará a los servicios pertinentes de la Comisión; a las instituciones, órganos y organismos pertinentes de la Unión; o a las autoridades competentes de los Estados miembros, a menos que para la ENISA resulte evidente que la aplicación de una limitación está prevista en uno de los actos a que se hace referencia en dichas letra s).

4. Toda limitación deberá ser necesaria y proporcionada teniendo en cuenta los riesgos para los derechos y las libertades de los interesados y el respeto, en lo esencial, de los derechos y libertades fundamentales en una sociedad democrática.

5. Si se estudia aplicar una limitación, deberá llevarse a cabo una evaluación de la necesidad y la proporcionalidad basada en las presentes normas. Esta se documentará con una nota interna de evaluación para cumplir con la obligación de rendir cuentas en cada caso.

6. Las limitaciones se levantarán tan pronto como dejen de cumplirse las circunstancias que las hubieran justificado; en particular, cuando se considere que el ejercicio del derecho limitado ya no anula el efecto de la limitación impuesta ni afecta negativamente a los derechos o las libertades de los demás interesados.

Artículo 4

Revisión por parte del responsable de la protección de datos

1. La ENISA informará al responsable de protección de datos de la agencia (en lo sucesivo, «RPD»), sin dilaciones indebidas, de toda situación en que el responsable del tratamiento limite la aplicación de los derechos de los interesados o prorrogue la limitación de conformidad con la presente Decisión. El responsable del tratamiento proporcionará al RPD acceso al registro que contenga la evaluación de la necesidad y la proporcionalidad de la limitación y documentará en dicho registro la fecha de la notificación al RPD. La ENISA deberá involucrar al RPD en los procedimientos pertinentes y la intervención de este último deberá documentarse.

2. El RPD podrá solicitar por escrito al responsable del tratamiento que revise la aplicación de las limitaciones. Este notificará por escrito al RPD el resultado de la revisión solicitada.

⁽³⁾ 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).

⁽⁴⁾ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

3. El responsable del tratamiento notificará al RPD el levantamiento de las limitaciones.

Artículo 5

Comunicación de información al interesado

1. En los casos debidamente justificados y en las condiciones estipuladas en la presente Decisión, el responsable del tratamiento podrá limitar el derecho a la información en el contexto de las siguientes operaciones de tratamiento:

- a) la realización de investigaciones administrativas y los procedimientos disciplinarios;
- b) las actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF;
- c) los procedimientos de denuncia de irregularidades;
- d) los procedimientos (formales e informales) en casos de acoso;
- e) las tramitaciones de quejas internas y externas;
- f) las auditorías internas;
- g) las investigaciones realizadas por el RPD en línea con lo dispuesto en el artículo 45, apartado 2, del Reglamento n.º 2018/1725;
- h) las investigaciones sobre la seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE);
- i) evaluaciones de incidentes de ciberseguridad realizadas por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, de acuerdo con el artículo 3, apartado 2, de la presente Decisión.

En los avisos de protección de datos, las declaraciones de confidencialidad o los registros, en el sentido del artículo 31 del Reglamento (UE) n.º 2018/1725, publicados en el sitio web o en la intranet de la ENISA, donde se informe a los interesados de sus derechos en el marco de determinado procedimiento, la ENISA incluirá información sobre la posible limitación de dichos derechos. Esta información abarcará los derechos que pueden limitarse, las razones de la limitación y la posible duración de esta.

2. Sin perjuicio de lo dispuesto en el apartado 3 del presente artículo, cuando resulte proporcionado, la ENISA también notificará de manera individualizada a todos los titulares de datos que se consideren interesados en la operación de tratamiento concreta cuáles son sus derechos con respecto a las limitaciones presentes o futuras, sin dilaciones indebidas y por escrito.

3. Cuando la ENISA limite, total o parcialmente, la comunicación de información a los interesados a que se refiere el apartado 2 del presente artículo, hará constar los motivos de la limitación y el fundamento jurídico con arreglo al artículo 3 de la presente Decisión, incluida una evaluación de la necesidad y la proporcionalidad de la limitación.

La consignación y, en su caso, los documentos que contengan los elementos de hecho y de derecho subyacentes se registrarán. Previa solicitud, se pondrán a disposición del Supervisor Europeo de Protección de Datos.

4. La limitación a que se refiere el apartado 3 del presente artículo seguirá aplicándose mientras persistan los motivos que la justifiquen.

Cuando desaparezcan los motivos que justifiquen la limitación, la ENISA informará al interesado de los principales motivos en que se hubiera basado la aplicación de la limitación. Al mismo tiempo, la ENISA informará al interesado del derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos en cualquier momento o a interponer un recurso ante el Tribunal de Justicia de la Unión Europea.

La ENISA revisará la aplicación de la limitación cada seis meses desde la fecha de su adopción y al cierre de la investigación o el procedimiento pertinentes. Posteriormente, el responsable del tratamiento deberá supervisar cada seis meses la necesidad de mantener cualquier limitación.

Artículo 6

Derecho de acceso del interesado

1. En los casos debidamente justificados y en las condiciones estipuladas en la presente Decisión, el responsable del tratamiento podrá limitar el derecho de acceso, cuando resulte necesario y proporcionado, en el contexto de las siguientes operaciones de tratamiento:

- a) la realización de investigaciones administrativas y los procedimientos disciplinarios;
- b) las actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF;
- c) los procedimientos de denuncia de irregularidades;

- d) los procedimientos (formales e informales) en casos de acoso;
- e) las tramitaciones de quejas internas y externas;
- f) las auditorías internas;
- g) las investigaciones realizadas por el RPD en línea con lo dispuesto en el artículo 45, apartado 2, del Reglamento n.º 2018/1725;
- h) las investigaciones sobre la seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE);
- i) evaluaciones de incidentes de ciberseguridad realizadas por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, de acuerdo con el artículo 3, apartado 2 de la presente Decisión.

Cuando los interesados soliciten el acceso a sus datos personales tratados en el contexto de uno o varios casos específicos o a una determinada operación de tratamiento, de conformidad con el artículo 17 del Reglamento (UE) n.º 2018/1725, la ENISA deberá circunscribir su evaluación de la solicitud exclusivamente a dichos datos personales.

2. Cuando la ENISA limite, en su totalidad o en parte, el derecho de acceso a que se refiere el artículo 17 del Reglamento (UE) n.º 2018/1725, deberá adoptar las siguientes medidas:

- a) informará al interesado, en su respuesta a la solicitud, de la limitación y de los principales motivos de esta, así como de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos o de interponer un recurso ante el Tribunal de Justicia de la Unión Europea;
- b) documentará en una nota interna de evaluación los motivos de la limitación, incluida una evaluación de la necesidad, la proporcionalidad y la duración de la limitación.

La comunicación de la información mencionada en la letra a) podrá aplazarse, omitirse o denegarse en caso de que pudiera dejar sin efecto la limitación, con arreglo a lo dispuesto en el artículo 25, apartado 8, del Reglamento (UE) n.º 2018/1725.

La ENISA revisará la aplicación de la limitación cada seis meses desde la fecha de su adopción y al cierre de la investigación. Posteriormente, el responsable del tratamiento deberá supervisar cada seis meses la necesidad de mantener cualquier limitación.

3. La consignación y, en su caso, los documentos que contengan los elementos de hecho y de derecho subyacentes se registrarán. Se pondrán a disposición del Supervisor Europeo de Protección de Datos, previa solicitud.

Artículo 7

Derecho de rectificación, supresión y limitación del tratamiento de datos

1. En los casos debidamente justificados y en las condiciones estipuladas en la presente Decisión, el responsable del tratamiento podrá limitar el derecho de rectificación, supresión y limitación, cuando resulte necesario y proporcionado, en el contexto de las siguientes operaciones de tratamiento:

- a) la realización de investigaciones administrativas y los procedimientos disciplinarios;
- b) las actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF;
- c) los procedimientos de denuncia de irregularidades;
- d) los procedimientos (formales e informales) en casos de acoso;
- e) las tramitaciones de quejas internas y externas;
- f) las auditorías internas;
- g) las investigaciones realizadas por el RPD en línea con lo dispuesto en el artículo 45, apartado 2, del Reglamento (UE) n.º 2018/1725;
- h) las investigaciones sobre la seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE);
- i) evaluaciones de incidentes de ciberseguridad realizadas por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, de acuerdo con el artículo 3, apartado 2 de la presente Decisión.

2. Cuando la ENISA limite, total o parcialmente, el ejercicio del derecho de rectificación, supresión o limitación del tratamiento a que se refieren el artículo 18; el artículo 19, apartado 1; y el artículo 20, apartado 1, del Reglamento (UE) n.º 2018/1725, adoptará las medidas contempladas en el artículo 6, apartado 2, de la presente Decisión y de conformidad con lo dispuesto en su artículo 6, apartado 3.

*Artículo 8***Comunicación de una violación de la seguridad de los datos personales al interesado y confidencialidad de las comunicaciones electrónicas**

1. En los casos debidamente justificados y en las condiciones estipuladas en la presente Decisión, el responsable del tratamiento podrá limitar el derecho a la comunicación de una violación de la seguridad de los datos personales, cuando resulte necesario y proporcionado, en el contexto de las siguientes operaciones de tratamiento:

- a) la realización de investigaciones administrativas y los procedimientos disciplinarios;
- b) las actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF;
- c) los procedimientos de denuncia de irregularidades;
- d) las tramitaciones de quejas internas y externas;
- e) las auditorías internas;
- f) las investigaciones realizadas por el RPD en línea con lo dispuesto en el artículo 45, apartado 2, del Reglamento (UE) n.º 2018/1725;
- g) las investigaciones sobre la seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE);
- h) evaluaciones de incidentes de ciberseguridad realizadas por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, de acuerdo con el artículo 3, apartado 2 de la presente Decisión.

2. En los casos debidamente justificados y en las condiciones estipuladas en la presente Decisión, el responsable del tratamiento podrá limitar el derecho a la confidencialidad de las comunicaciones electrónicas, cuando resulte necesario y proporcionado, en el contexto de las siguientes operaciones de tratamiento:

- a) la realización de investigaciones administrativas y los procedimientos disciplinarios;
- b) las actividades preliminares relacionadas con casos de posibles irregularidades puestas en conocimiento de la OLAF;
- c) los procedimientos de denuncia de irregularidades;
- d) los procedimientos formales en casos de acoso;
- e) las tramitaciones de quejas internas y externas;
- f) las investigaciones sobre la seguridad (informática) realizadas internamente o con la participación de agentes externos (por ejemplo, CERT-UE).
- g) evaluaciones de incidentes de ciberseguridad realizadas por la ENISA con arreglo al artículo 7, apartado 4, del Reglamento (UE) n.º 2019/881, de acuerdo con el artículo 3, apartado 2.

3. Cuando la ENISA limite la comunicación de una violación de la seguridad de los datos personales al interesado o la confidencialidad de las comunicaciones electrónicas a que se refieren los artículos 35 y 36 del Reglamento (UE) n.º 2018/1725, deberá aplicar las disposiciones del artículo 5, apartado 3, de la presente Decisión. Será de aplicación el artículo 5, apartado 4, de la presente Decisión.

*Artículo 9***Entrada en vigor**

La presente Decisión entrará en vigor al día siguiente de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Atenas, el 21 de noviembre de 2019.

Por la ENISA
Jean Baptiste DEMAISON
Presidente del Consejo de Administración
