DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno Nº 36 | Junio 2023

PROTECCIÓN DE DATOS DE LAS PERSONAS INFORMANTES SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN

Í N D I C E

PROTECCIÓN DE DATOS DE LAS PERSONAS INFORMANTES SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

INTRODUCCIÓN

Con la aprobación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción se transpone, esto es, se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.

La norma europea permite a los Estados eximir de la implantación del canal interno a los municipios de menos de 10.000 habitantes o entidades del sector público de menos de 50 trabajadores. Sin embargo, la Ley 2/2023, al enunciar el ámbito de aplicación en su artículo 13, ha prescindido de esta opción.

"Con la aprobación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción se transpone, esto es, se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019".

A través del sistema interno de información, se podrá informar ante una hipotética infracción de legislación o normativa, referida, entre otros, a:

- Contratación pública.
- Servicios, productos y medios financieros y prevención del blanqueo de capitales y la financiación del terrorismo.
- Seguridad del transporte
- Protección del medio ambiente.
- Cadena alimentaria, y en particular en la seguridad de los alimentos y los piensos, así como de la sanidad, la protección y el bienestar de los animales.

"La citada directiva regula aspectos mínimos que debían abarcar los distintos cauces de información a través de los cuales una persona conocedora de una infracción del derecho de la Unión Europea pueda dar a conocer la existencia de la misma en un entorno laboral".

- Protección de los usuarios o consumidores.
- Protección de la intimidad y los datos personales.
- Seguridad de las redes y los sistemas de información

En el presente cuaderno, en primer lugar, se indica cuál es el ámbito personal de aplicación, así como que entidades del sector público están obligadas a crear un sistema interno de información. A continuación, se muestran los principales requisitos o características que debe reunir el sistema de interno de información; coloquialmente conocido como canal de denuncias o *whistleblowing.*

Por otra parte, se citan las principales actuaciones, de conformidad con la legislación en protección de datos de carácter personal, que deberán llevar a cabo los entes públicos, como responsables del tratamiento de los datos personales de los informantes, así como del resto de personas involucradas en la comunicación efectuada por éstos.

Además de tales canales internos, exige la Directiva la determinación de otros canales de información, denominados «externos», con el fin de ofrecer a los ciudadanos una comunicación con una autoridad pública especializada, lo que les puede generar más confianza al disipar su temor a sufrir alguna represalia en su entorno.

Por último, se indica el papel del Delegado de Protección de Datos en relación con los tratamientos de datos personales llevados a cabo a través del Sistema interno de información o canal de denuncias interno.

ÁMBITO DE APLICACIÓN DE LA LEY DE PROTECCIÓN DE LOS INFORMANTES

1. Ámbito de aplicación personal.

Esta Ley se aplicará a las personas físicas informantes, que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

a) las personas que tengan la condición de empleados públicos o trabajadores por cuenta ajena;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

También se aplicará a los informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

"La Ley protege a las personas físicas informantes, que trabajen en el sector público y que hayan obtenido información sobre infracciones en un contexto laboral".

2. Entidades obligadas en el sector público.

Por otra parte, la Ley dispone que todas las entidades que integran el sector público estarán obligadas a disponer de un Sistema interno de información en los términos que marca la ley, tales como:

> a) La Administración General del Estado, las Administraciones de las comunidades autónomas, ciudades con Estatuto de Autonomía y las **entidades que integran la Administración Local.**

b) **Los organismos y entidades públicas vinculadas o dependientes** de alguna Administración pública, **así como aquellas otras asociaciones y corporaciones en las que participen** Administraciones y organismos públicos.

Estas entidades serán responsables del tratamiento de datos de carácter personal de las personas informantes.

"Todas las entidades que integran el sector público estarán obligadas a disponer de un Sistema interno de información".

PRINCIPALES CARACTERÍSTICAS DEL SISTEMA INTERNO DE INFORMACIÓN

La Ley contiene unas disposiciones generales sobre las características o requisitos que deberá cumplir el canal de denuncias interno, que se aplicarán tanto a sector público como privado. Entre estas, a continuación, se citan las principales:

1. Se impone la **obligación de realizar consulta previa con los sindicatos y representación legal de los trabajadores (empleados públicos)**, a quienes se les reserva por tanto un papel relevante en la configuración del canal (artículo 5.1.)

2. El órgano de **administración** o de gobierno tendrá la **condición de responsable del tratamiento de los datos personales** que sean objeto de tratamiento durante las denuncias (artículo 5.1)

"El órgano de administración o de gobierno tendrá la condición de responsable del tratamiento de los datos personales que sean objeto".

3. En su artículo 5.2.b) la ley impone que el sistema garantice la **confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación** y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, la protección de datos, impidiendo el acceso de personal no autorizado. Aquellas personas a las que se refieran los hechos relatados en la comunicación, efectuada por el informante, han de contar con una singular protección ante el riesgo de que la información, aun con aparentes visos de veracidad, haya sido manipulada, sea falsa o responda a motivaciones que el Derecho no puede amparar. Estas personas mantienen todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia

4. Se debe permitir la **presentación de comunicaciones por escrito o verbalmente**, o de ambos modos (artículo 5.2.c)

5. En el caso de existir diferentes canales internos de denuncia, estos deberán integrarse y estar disponibles de manera unificada en la página principal del espacio web de la entidad, **en una sección separada y fácilmente identificable.** Además, el canal

de denuncias y su funcionamiento deben ser transparentes, obligando a publicar información de forma clara y fácilmente accesible sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión (artículo 5.2.d).

6. Deben ser **independientes** y estar **diferenciados del resto de sistemas de información** de otras entidades u organismos (artículo 5.2.f).

7. Debe existir un **procedimiento de gestión** de las informaciones recibidas (artículo 5.2.i).

8. Los **canales** de comunicación deben ser **claros, públicos y de fácil acceso** a empleados y terceros que deseen interponer una comunicación.

"El sistema debe garantizar la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, la protección de datos, impidiendo el acceso de personal no autorizado".

"La Administración pública deberá adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado".

OBLIGACIONES DE LA ADMINISTRACIÓN PÚBLICA, RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES DE LOS INFORMANTES

Sin entrar, de manera exhaustiva y pormenorizada, en todas las actuaciones que debe acometer la Administración pública, como responsable del tratamiento de los datos personales de los informantes y demás personas involucradas, a continuación, se indican las más relevantes:

1. La Administración pública debe diseñar, establecer y gestionar de una forma segura el sistema interno de información. De modo que, dicho sistema garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

2. La Administración pública, en calidad de responsable del tratamiento, deberá adoptar las **medidas** necesarias **para preservar la identidad y garantizar la confidencialidad** de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

Esto supone la adopción de **medidas de seguridad, técnicas y organizativas**, en el sistema de información. De acuerdo con la Disposición adicional primera de la LOPDGDD, las medidas de seguridad serán conforma al Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad (ENS).**

3. No obstante, antes de adoptar las medidas, dado que, por la naturaleza como por el contexto, supone un tratamiento de datos de carácter personal de alto riesgo para los derechos y libertades de las personas físicas informantes, de conformidad con el articulo 35 RGPD, la Administración pública, en calidad de responsable del tratamiento, deberá realizar una **Evaluación de Impacto en Protección de Datos (EIPD).**

"En el caso de que se contrate a un tercero externo, para la gestión y mantenimiento del sistema de información, la Administración pública deberá formalizar el encargo de tratamiento de datos personales. Este tercero tendrá la obligación, a prever en Pliego o contrato, de adoptar las medidas de seguridad del Esquema Nacional de Seguridad".

4. En el caso de que se contrate a un tercero externo, para la gestión y mantenimiento del sistema de información, la Administración pública deberá formalizar, de conformidad con el artículo 28 RGPD y artículo 33 LOPDGDD, el **encargo de tratamiento de datos personales**. Este tercero, en calidad de encargado de tratamiento, tendrá la obligación, a prever en Pliego o contrato, de adoptar las medidas de seguridad del Esquema Nacional de Seguridad.

5. Los datos personales de quien formule la comunicación y de los empleados y terceros **deberán conservarse** en el sistema de denuncias únicamente **durante el tiempo imprescindible** para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

6. En todo caso, transcurridos 3 meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

7. La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

CANAL EXTERNO DE INFORMACIÓN A.A.I.

"Toda persona física podrá informar también ante la Autoridad Independiente de Protección del Informante (A.A.I.). En el ámbito de la Comunidad Valenciana, adicionalmente (pero no en sustitución del canal de la A.A.I.), podrá utilizarse el buzón externo de denuncias de la Agencia Valenciana Antifraude".

El sistema interno de información debe ser complementado con un canal externo, es decir, con la posibilidad de que quien conozca el hecho susceptible de ser comunicado con arreglo a esta norma pueda acudir a una autoridad pública que, con todas las garantías, tenga constancia del hecho informado y proceda a investigarlo y, en su caso, pueda colaborar con el Ministerio Fiscal cuando aprecie que el hecho objeto de la comunicación es constitutivo de delito.

De este modo, **toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes**, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de esta ley, ya sea directamente o previa comunicación a través del correspondiente canal interno.

La información **se podrá realizar por escrito, a través de correo postal o a través de cualquier medio electrónico** habilitado al efecto dirigido al canal externo de informaciones de la A.A.I., o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial, dentro del plazo máximo de siete días. En los casos de comunicación verbal se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con el artículo 13 RGPD y 11 LOPDGDD.

En el ámbito de la Comunidad Valenciana, adicionalmente (pero no en sustitución del canal de la A.A.I.), podrá utilizarse el buzón externo de denuncias de la Agencia Valenciana Antifraude y, en todo caso, se utilizará para comunicar irregularidades contrarias a la integridad pública o potencialmente constitutivas de fraude o corrupción de ámbito autonómico

"A su vez, convive con otros canales de denuncias externos como el habilitado por el SNCA (Infofraude), para la comunicación de información sobre fraudes o irregularidades que afecten a fondos europeos".

(incluyendo todo tipo de irregularidades para proteger toda clase de fondos públicos). Así, a los efectos de prácticas contrarias a la integridad, fraude y corrupción sobre fondos públicos podrá designarse como tal, al amparo de la Ley 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana, el buzón externo de denuncias de la Agencia Valenciana Antifraude.

A su vez, convive con otros canales de denuncias externos como el habilitado por el SNCA (Infofraude), para la comunicación de información sobre fraudes o irregularidades que afecten a fondos europeos, el cual dispone de un apartado específico relativo al Mecanismo de Recuperación y Resiliencia, teniendo en cuenta lo dispuesto en la Comunicación 1/2017, de 6 de abril, sobre la forma en la que pueden proceder las personas que tengan conocimiento de hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea.

EL PAPEL DEL DELEGADO DE PROTECCIÓN DE DATOS

El artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (**LOPDGDD**) establece únicamente los requisitos que deben tener los sistemas de información de denuncias internas, a fin de garantizar la privacidad de los denunciantes. Sin embargo, **nada nos dice acerca del nombramiento y designación de persona para el desempeño de Delegado de Protección de Datos (DPD) en las entidades obligadas a la creación de los sistemas internos de información.**

Pues bien, el Preámbulo de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, nos dice que *"Por otra parte, se exige que las entidades obligadas a disponer de un Sistema interno de información, los terceros externos que en su caso lo gestionen y la Autoridad Independiente de Protección de Datos, A.A.I. así como las que en su caso se constituyan, cuenten con un delegado de protección de datos".*

No obstante, esta obligación no se ha incluido en el articulado vigente de la Ley 2/2023. Únicamente, el artículo 34 de esta Ley, nos dice que *"De acuerdo con lo que dispone el artículo 37.1.a) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Autoridad Independiente de Protección del Informante, A.A.I., y las autoridades independientes que en su caso se constituyan, deberán nombrar un delegado de protección de datos".*

Antes de la aprobación de la vigente Ley, el Proyecto de Ley incluía, en su artículo 34, una referencia expresa a la obligación por parte de las entidades de nombrar un Delegado de Protección de Datos, que implicaba que todas las entidades privadas de más de 50 personas trabajadoras tuvieran que disponer de un DPD. No obstante, tal y como se ha recogido en el articulado finalmente aprobado, la Ley obliga

"El Delegado de Protección de Datos tendrá acceso a los datos personales contenidos en el Sistema interno de información, dentro del ámbito de sus competencias y funciones, exclusivamente".

"Como los sujetos del artículo 77.1 LOPDGDD (esto es, en términos generales, la Administración pública) está obligada a nombrar y designar un DPD, no tendrá la necesidad de nombrar otro DPD a los efectos del asesoramiento y supervisión de este sistema de información".

únicamente a la Autoridad Independiente de Protección del Informante (A.A.I.), y las autoridades independientes que en su caso se constituyan a nombrar un DPD; hecho que resulta contradictorio con lo dispuesto en el Preámbulo. Sin embargo, al no incluir, de forma expresa, esta obligación en el articulado vigente de la Ley se interpreta que se ha eliminado la obligación de designar un DPD, de manera general, para todas aquellas entidades que deban disponer de un Sistema Interno de información.

En todo caso, cabe decir que, como los sujetos del artículo 77.1 LOPDGDD (esto es, en términos generales, la **Administración pública**) está **obligada a nombrar y designar un DPD, no tendrá la necesidad de nombrar otro DPD, a los efectos del asesoramiento y supervisión de este sistema de información.**

Aclarado esto, **el papel del DPD será también el asesoramiento y supervisión**, como si de otra actividad de tratamiento de datos de carácter personal se tratase. Si bien, de conformidad con el artículo 32 de esta Ley 2/2023, el DPD también **tiene acceso a los datos personales contenidos en el sistema interno de información; limitado al ámbito de sus competencias y funciones.**

MATERIAL COMPLEMENTARIO

- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Consulta la Ley en este enlace.
- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Consulta la Directiva en este enlace.
- Publicación de la AEPD sobre "Privacidad en sistemas de denuncia o 'whistleblowing'. Consulta la Publicación en este enlace.

NOTICIAS

- **El Boletín Oficial del Estado (BOE) ha publicado una modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).**

  Después de varios años desde la aplicación del Reglamento General de Protección de Datos (RGPD) y la entrada en vigor de la Ley Orgánica, se han llevado a cabo modificaciones tanto en la tramitación de algunos procedimientos de la Agencia Española de Protección de Datos (AEPD) como en su Estatuto.

  Consulta la publicación en este enlace.

- **La Agencia Española de Protección de Datos (AEPD) ha publicado, en colaboración con la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) y la Asociación Profesional Española de Privacidad (APEP), la guía Orientaciones para la supervisión de sistemas criptográficos como medida de seguridad en protección de datos.**

  El documento recoge que el cifrado será una medida adecuada de seguridad para la protección de datos siempre que su implementación se ajuste a las características e impacto del tratamiento en los derechos y libertades de los afectados.

  Consulta la publicación en este enlace.