PROCEDIMIENTO y POLÍTICA PARA LA GESTIÓN DE INFORMACIONES 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

(CANAL DE DENUNCIAS)

ÍNDICE

PRINCIPIOS Y PROCEDIMIENTO PARA LA GESTIÓN DE INFORMACIONES 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 (CANAL DE DENUNCIAS)

1. CONCEPTO

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 ha venido a transponer a nuestro ordenamiento jurídico la Directiva 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.

La finalidad de la norma es la de proteger a las personas que en un contexto laboral o profesional detecten infracciones del Derecho de la Unión previstas en la Directiva del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, así como infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados en la misma y que se desarrollan en este Protocolo.

Este sistema para la comunicación de infracciones ha recibido nombres como canal de denuncias o whistleblowing.

La buena fe, la conciencia honesta de que se han producido o pueden producirse hechos graves perjudiciales constituye un requisito indispensable para la protección del informante. Esa buena fe es la expresión de su comportamiento cívico y se contrapone a otras actuaciones que, por el contrario, resulta indispensable excluir de la protección, tales como la remisión de informaciones falsas o tergiversadas, así como aquellas que se han obtenido de manera ilícita.

La protección amparada por la Ley se extiende a todas aquellas personas que tienen vínculos profesionales o laborales con la entidad, incluso aquellas que ya han finalizado su relación profesional, voluntarios, trabajadores en prácticas o en período de formación, personas que participan en procesos de selección, etc. También se extiende el amparo de la ley a las personas que prestan asistencia a los informantes, a las personas de su entorno que puedan sufrir represalias, así como a las personas jurídicas propiedad del informante, entre otras.

El Sistema interno de información de infracciones abarca tanto el canal, entendido como buzón o cauce para recepción de la información, como el Responsable del Sistema y el procedimiento. El Sistema interno de información deberá utilizarse de manera preferente para canalizar la información, pues una actuación diligente y eficaz en el seno de la propia organización podría paralizar las consecuencias perjudiciales de las actuaciones investigadas.

La configuración del Sistema interno de información debe reunir determinados requisitos, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante. Asimismo, resulta indispensable para la eficacia del Sistema interno de información la designación del responsable de su correcto funcionamiento.

Se ha de destacar que se permite la comunicación anónima. Además, la preservación de la identidad del informante es una de las premisas esenciales para garantizar la efectividad de la protección que persigue la Ley, de ahí que se exija que en todo momento deba ser garantizada. En esta línea se dispone que el dato de la identidad del informante nunca será objeto del derecho de acceso a datos personales y se limita la posibilidad de comunicación de dicha identidad sólo a la autoridad judicial, el Ministerio Fiscal o la autoridad administrativa competente exigiendo que en todo caso se impida el acceso por terceros a la misma.

Por su parte, el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales legitima el tratamiento de estos datos al disponer que "serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas." Concretamente la legitimación del tratamiento viene dada por el artículo 6.1 c) del RGPD. Se indica asimismo que en caso de que la persona investigada ejerza el derecho de oposición al tratamiento de sus datos personales se entiende que existen motivos legítimos imperiosos que legitiman continuar con dicho tratamiento, tal como permite el artículo 21.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Pero las medidas de protección no se dirigen sólo a favor de los informantes. También aquellas personas a las que se refieran los hechos relatados en la comunicación (denuncia) 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; en fin, de los mismos derechos que goza el informante.

La Ley regula igualmente la posibilidad de comunicar irregularidades a través de canales externos. Por tanto, cualquier persona física que desee informar una conducta irregular en el ámbito de la empresa podrá acudir indistintamente al canal interno, al canal externo o a ambos.

2. DEFINICIONES

Informante (denunciante): persona física o jurídica que haya obtenido información sobre infracciones en un contexto laboral o profesional y que las pongan en conocimiento de la Organización, comprendiendo en todo caso las previstas en el Articulo 3 apartados 1 y 2 de la Ley 2/2023.

Persona afectada (denunciada): persona física a la que se atribuye por el informante la comisión de las infracciones a las que se refiere el artículo 2 de la Ley 2/2023. También se considerarán personas afectadas, las que, sin haber sido objeto de información por el informante, a través de los actos de instrucción del procedimiento se haya tenido conocimiento de la presunta comisión por parte de éstas de las infracciones antes referenciadas.

Terceros: personas físicas que pueden tener conocimiento de aspectos relacionados con la infracción informada, ya sea como testigo directo o indirecto y que pueden aportar información al procedimiento.

Sistema interno de información: es el cauce de información establecido en la Organización para informar sobre las acciones u omisiones previstas en el artículo 2 de la Ley 2/2023, con las funciones y contenidos recogidos en el artículo 5.2 de dicha norma. Incluye el Canal interno de información y el Sistema de gestión de la información.

Canal interno de información: El canal específicamente habilitado por EXPORTADORA DATA BASE S.A. para recibir la información. Las informaciones recibidas por cualquier medio en la organización, relacionadas con el objeto de este procedimiento, se remitirán al canal interno de información, que se crea en la organización bajo la administración del Responsable del Sistema Interno de información de la misma.

Sistema de gestión de la Información: plataforma tecnológica integrada en el Sistema interno de información, cuya finalidad es la llevanza, registro y conservación de las actuaciones que tengan lugar como consecuencia de la presentación una información a la que sea aplicable la Ley 2/2023.

Canal externo de información: 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 la ley, ya sea directamente o previa comunicación a través del correspondiente canal interno.

3. OBJETIVOS DEL SISTEMA INTERNO PARA LA COMUNICACIÓN DE INFRACCIONES

Los objetivos perseguidos con la implantación de un sistema interno de información son:

- Prevenir la realización de conductas que supongan infracciones del Derecho de la Unión previstas en la Directiva del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 e infracciones penales o administrativas graves o muy graves, así como el propio código de conducta de la organización.
- Detectar de forma temprana la comisión de conductas que pudieren constituir delito o infracción de las mencionadas en el punto anterior.
- Evitar la comisión de infracciones y delitos en el seno de la organización o minimizar sus efectos.
- Garantizar el anonimato, la confidencialidad y la indemnidad de la persona informante frente a posibles represalias.
- Implementar una cultura de cumplimiento, transparencia, información y buenas prácticas en la organización.
- Dotar a la organización de mecanismos de conocimiento y control de las eventuales conductas de incumplimiento.
- Generar el proceso disciplinario y de imposición de sanciones a los autores de las conductas infractoras.
- En su caso, colaborar con la administración de justicia o la administración pública competente.

4. PRINCIPIOS DEL SISTEMA INTERNO DE INFORMACIÓN DE INFRACCIONES

El sistema interno de información de infracciones debe cumplir con las siguientes garantías:

- **Confidencialidad**. Se utilizarán sistemas de comunicación que sean eficaces y garanticen que se preserve la confidencialidad de lo informado y de las personas implicadas, incluida la persona sobre la que se informa.

Es esencial que la persona informante goce de una protección apropiada, garantizando la privacidad de la información e impidiendo que pueda ser identificada, lo que es fundamental para cumplir con el cometido del canal de información de infracciones y para que se fomente su uso.

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.

- **Forma.** Se permite la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.
- **Anonimato del informante**. 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 permite que la denuncia sea anónima. En el caso de que la denuncia no sea anónima, se garantizará la confidencialidad de la identidad del informante y de las personas implicadas.
- **Indemnidad del informante**. Se garantiza que no serán tomadas represalias contra el denunciante o informante.
  Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública. En particular, se consideran represalias, sin carácter exhaustivo, las que se adopten en forma de: despido, degradaciones o denegaciones de ascensos, modificaciones sustanciales de las condiciones de trabajo, daños, coacciones, amenazas, intimidaciones, acoso, inclusión en listas negras, denegación de formación, discriminación, etc.
- **Derechos de la persona afectada (denunciada).** Derecho a que se le informe de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento. Respeto a la presunción de inocencia y al honor de las personas denunciadas. Derecho a la confidencialidad de su identidad. Derecho a estar asistido por abogado.
- **Información**. Deberá informarse a todos los miembros de la organización y colaboradores de la existencia y el funcionamiento del sistema interno de información de infracciones, la confidencialidad, el anonimato, la indemnidad del informante y que el acceso a dicho canal está restringido y solo será accesible al órgano o persona designada por la empresa como Responsable del Sistema.

- **Evaluación**. Deberá realizarse una evaluación periódica del funcionamiento del Sistema de Información de Infracciones a través de un procedimiento de mejora continua.
- **Responsable del Sistema Interno de Información.** Es la persona u órgano colegiado encargada de la gestión y la tramitación de los expedientes de investigación. Deberá desarrollar sus funciones de forma independiente y autónoma (siempre que sea posible debido a la naturaleza y dimensiones de la empresa).
- **Establecimiento de un régimen disciplinario**. Para sancionar a los autores de las conductas prohibidas.
- **Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito.**

5. PROCEDIMIENTO DE TRAMITACIÓN DE COMUNICACIONES

a) ¿Qué es el canal de comunicaciones (denuncias)? Es la vía de comunicación interna que permite al informante poner en conocimiento de la organización cualquier posible conducta ilícita o irregular de la que haya sido testigo o tenga conocimiento. Es por tanto una herramienta que permite detectar comportamientos irregulares o ilícitos dentro de la organización. A través del canal de denuncias interno, los miembros de la organización y aquellas personas ajenas a la misma pero que se relacionen con ella (informantes) pueden denunciar esos comportamientos dando oportunidad a la organización para que pueda resolverlos internamente de manera temprana o poner los hechos en conocimiento de las autoridades competentes cuando son constitutivos de delitos. Se trata de una comunicación dirigida al Responsable del Sistema Interno de Información.

b) ¿Qué conductas irregulares se pueden informar a través del canal?

1. Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea dentro del ámbito del anexo de la 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 y siempre que afecten a los intereses financiares de la Unión Europea e incidan en el mercado interior. El ámbito del mencionado anexo de la Directiva incluye las siguientes categorías:

   i) contratación pública;

ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo;
iii) seguridad de los productos y conformidad;
iv) seguridad del transporte;
v) protección del medio ambiente;
vi) protección frente a las radiaciones y seguridad nuclear;
vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales;
viii) salud pública;
ix) protección de los consumidores;
x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información;

2. Acciones u omisiones que puedan ser constitutivas de infracción penal.
3. Acciones u omisiones que puedan ser constitutivas de infracciones administrativas graves o muy graves.
4. Acciones u omisiones que sean contrarias a la política de la organización.

A título de ejemplo, sin carácter exhaustivo, son conductas irregulares:

- Delitos contra la Hacienda Pública y la Seguridad Social o infracciones administrativas graves o muy graves que impliquen quebranto económico a estas.
- Administración desleal.
- Estafas.
- Delitos relativos al mercado y a los consumidores.
- Delitos de corrupción en los negocios.
- Delitos societarios.
- Receptación y blanqueo de capitales.
- Delitos contra los derechos de los trabajadores e infracciones administrativas graves o muy graves que afecten a los derechos de estos.
- Delitos contra el medio ambiente e infracciones administrativas graves o muy graves que afecten al mismo.
- Cohecho
- Descubrimiento y revelación de secretos.
- Hechos que puedan constituir infracciones administrativas graves o muy graves por incumplimiento de la normativa sobre protección de datos.
- Fraude a los presupuestos generales de la Unión Europea.

La finalidad de canal de comunicaciones no es la de informar sobre sugerencias, quejas, comentarios, recomendaciones o consultas acerca de la actividad de la organización.

c) **¿Quién puede informar a través del canal?** Son informantes:

- Personas que tienen vínculos profesionales o laborales con la entidad.
- Aquellas personas que ya han finalizado la relación profesional.
- Trabajadores y alumnos en prácticas.
- Personas que participan en procesos de selección de personal.
- Autónomos.
- Accionistas, socios, miembros del órgano de dirección, administración de la entidad.
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

d) **¿Cómo se puede informar de una conducta irregular?** La persona informante podrá realizar la comunicación por escrito, verbalmente o de ambas maneras. Para ello nuestra organización pone a su disposición los siguientes medios:

SI DESEA REALIZAR UNA DENUNCIA ANÓNIMA:

- Puede enviar su comunicación anónima a la dirección postal **C/DOÑANA 1 28924 ALCORCON (MADRID)** dirigiendo la misma al Responsable del Sistema Interno de Información.

NOTA: Si la denuncia se presenta de forma anónima y se remite por este medio, no será posible realizar el seguimiento ni recibir información sobre su tramitación, salvo que la persona informante facilite, dentro de la propia comunicación, un medio de contacto que preserve su anonimato.

SI DESEA REALIZAR UNA DENUNCIA IDENTIFICÁNDOSE:

- Puede enviar sus comunicaciones, identificándose, a la dirección de correo electrónico **administracion@edb.es**

- Puede enviar su comunicación, identificándose, a la dirección postal **C/DOÑANA 1 28924 ALCORCON (MADRID)** dirigiendo la misma al Responsable del Sistema Interno de Información.

- Presencialmente ante el Responsable del Sistema Interno de Información. La reunión tendrá lugar en un plazo máximo de siete días desde su solicitud a través de la dirección de email **administracion@edb.es**

En cualquier caso, la persona informante deberá describir de forma detallada las conductas de las que tenga conocimiento y sobre las que quiera informar y que pueden constituir una irregularidad, la fecha en que tuvieron lugar los hechos, indicar la identidad de la persona presuntamente infractora, el centro y puesto en los que trabaja (en su caso) y aportar cuantas pruebas estén a su disposición.

En el caso de que la comunicación se realice verbalmente (por teléfono, mediante reunión presencial, etc.) la información se documentará, previo consentimiento del informante, mediante su grabación en formato seguro, duradero y accesible o a través de su transcripción completa y exacta (ofreciendo al informante la posibilidad de comprobar, rectificar y firmar la transcripción).

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones. No obstante, se admiten las comunicaciones realizadas de forma anónima. En su caso, se enviará al informante acuse de recibo de la comunicación en un plazo máximo de siete días naturales.

Para el caso de que el informante desee presentar una queja / denuncia sobre una conducta relativa a acoso moral, sexual y por razón de sexo, la violencia sexual o la discriminación del colectivo LGTBI, se deberá proceder a su presentación a través del buzón habilitado por la empresa al efecto, conforme al procedimiento recogido en el protocolo de acoso moral, sexual y por razón de sexo, la violencia sexual o la discriminación del colectivo LGTBI.

e) ¿Es necesario identificarse para comunicar una infracción? No, son admisibles las comunicaciones anónimas.

f) **¿Quién es el Responsable del Sistema Interno de Información?** El Responsable del Sistema Interno de Información es la persona u órgano colegiado designado por sus cualidades por la organización para la gestión del Sistema Interno de Información (incluyendo la recepción de comunicaciones y la tramitación de expedientes).

Es la persona u órgano colegiado a quien se dirige el informante para la recepción y tramitación de la información comunicada.

En el caso de nuestra organización, la persona designada como Responsable del Sistema Interno de Información es la persona que ocupa el **cargo responsable de administración y personal en la empresa.**

Plazo para notificar a la A.A.I. el nombramiento/cese del Responsable del Sistema:

Tanto el nombramiento como el cese (y las razones que han justificado el cese), en su caso, de la persona designada como Responsable del Sistema Interno de Información deberán ser notificadas en el **plazo de 10 días hábiles** a la Autoridad Independiente de Protección del Informante (A.A.I) o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias.

g) **¿Qué ocurre si la recepción de la información se produce por personas ajenas al Responsable del Sistema Interno?**

Cuando la información no se remita a través del canal interno de información y llegue a miembros de la organización distintos del Responsable del Sistema, éstos tienen la obligación de remitírsela a este Responsable con carácter inmediato, así como el deber de preservar su confidencialidad y abstenerse de realizar cualquier actuación que pueda revelar directa o indirectamente la identidad del informante y de la persona afectada.

La divulgación por parte del tercero receptor de la mera existencia y, en su caso, del contenido de la información, puede suponer la vulneración de las garantías de confidencialidad y anonimato, conducta tipificada como infracción muy grave en el artículo 63.1. c) de la Ley 2/2023.

h) ¿Son seguros los canales de comunicación respecto a la confidencialidad de la identidad de las personas implicadas y la información comunicada?

1. Confidencialidad de la identidad de la persona informante:

El canal está diseñado, establecido y gestionado de forma segura, garantizando la confidencialidad de la identidad del informante, así como la protección de los datos a los que se refiere la información, por lo que se impide el acceso a la misma por parte del personal no autorizado. Esto se aplicará a cualquier dato del que se pueda deducir directa o indirectamente la identidad del informante. La identidad de los informantes será en todo caso reservada, lo que implica que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

La identidad del informante sólo podrá ser comunicada, en el caso de que resulte legalmente exigible, a la Autoridad judicial, a la Fiscalía correspondiente o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, lo que se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

2. Confidencialidad de la identidad de la persona a la que se refiera la información

A la persona a la que se refiere la información comunicada (persona denunciada) se le garantiza la confidencialidad de sus datos personales con el objeto de evitar la posible difusión de los mismos. A estos efectos, el canal de información está diseñado, establecido y gestionado de forma segura, garantizando la confidencialidad de la identidad de la persona afectada por la información y la protección de los hechos y datos del procedimiento, por lo que se impide el acceso a la información por parte del personal no autorizado.

i) ¿Cómo se tramitan los expedientes de comunicaciones?

Al recibir la comunicación, el Responsable del Sistema Interno de Información asignará un código numérico al expediente para su identificación y seguimiento y se enviará acuse de recibo al informante en un plazo máximo de siete días naturales, a menos que el informante haya renunciado expresamente a recibir notificaciones o se trate de

un informante anónimo que haya remitido una comunicación postal o de otra manera que no permita ese acuse de recibo.

Seguidamente, el Responsable del Sistema Interno de Información realizará una evaluación previa del contenido de la comunicación a fin de definir el tipo de infracción en que se encuadra la información comunicada o si debe inadmitirla a trámite.

El Responsable remitirá la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea o el órgano que resulte competente.

Cuando se traten de infracciones administrativas graves o muy graves se podrán remitir a la autoridad competente para su tramitación.

El Responsable podrá inadmitir a trámite la comunicación en los siguientes supuestos:

- Cuando los hechos relatados carezcan de toda verosimilitud.
- Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de la Ley, salvo que se trate de hechos constitutivos de conductas contrarias a las normas corporativas de las que se puedan derivar un procedimiento disciplinario.

Una vez admitida a trámite la comunicación, se iniciará la fase de instrucción del expediente que comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

Se mantendrá una entrevista con la persona afectada (es decir, la persona investigada frente a la que se dirige la comunicación remitida por el informante) y se le informará de las acciones u omisiones que se le atribuyen, y de su derecho a ser oída en cualquier momento y de su derecho a estar asistida de abogado. Dicha comunicación tendrá lugar en el plazo máximo de 15 días desde la resolución de admisión, salvo que dicha comunicación pueda facilitar la ocultación, destrucción y alteración de pruebas, en cuyo caso, el Responsable del Sistema Interno, de forma motivada, podrá modificar dicho plazo hasta que desaparezcan dichas circunstancias. En todo caso se respetará el derecho a la presunción de inocencia y al honor de la persona afectada.

En ningún caso se comunicará a los sujetos afectados (denunciados) la identidad del informante ni se dará acceso a la comunicación.

Los actos de comunicación y entrevistas que, en su caso procedan, se realizarán con la máxima discreción posible, con la finalidad de preservar el secreto de las actuaciones, preservando la identidad del informante, terceros y afectados y, en todo caso, garantizando la confidencialidad de las informaciones.

Durante esta fase de instrucción se podrán adoptar las medidas cautelares que se consideren razonables y proporcionadas por parte del Responsable.

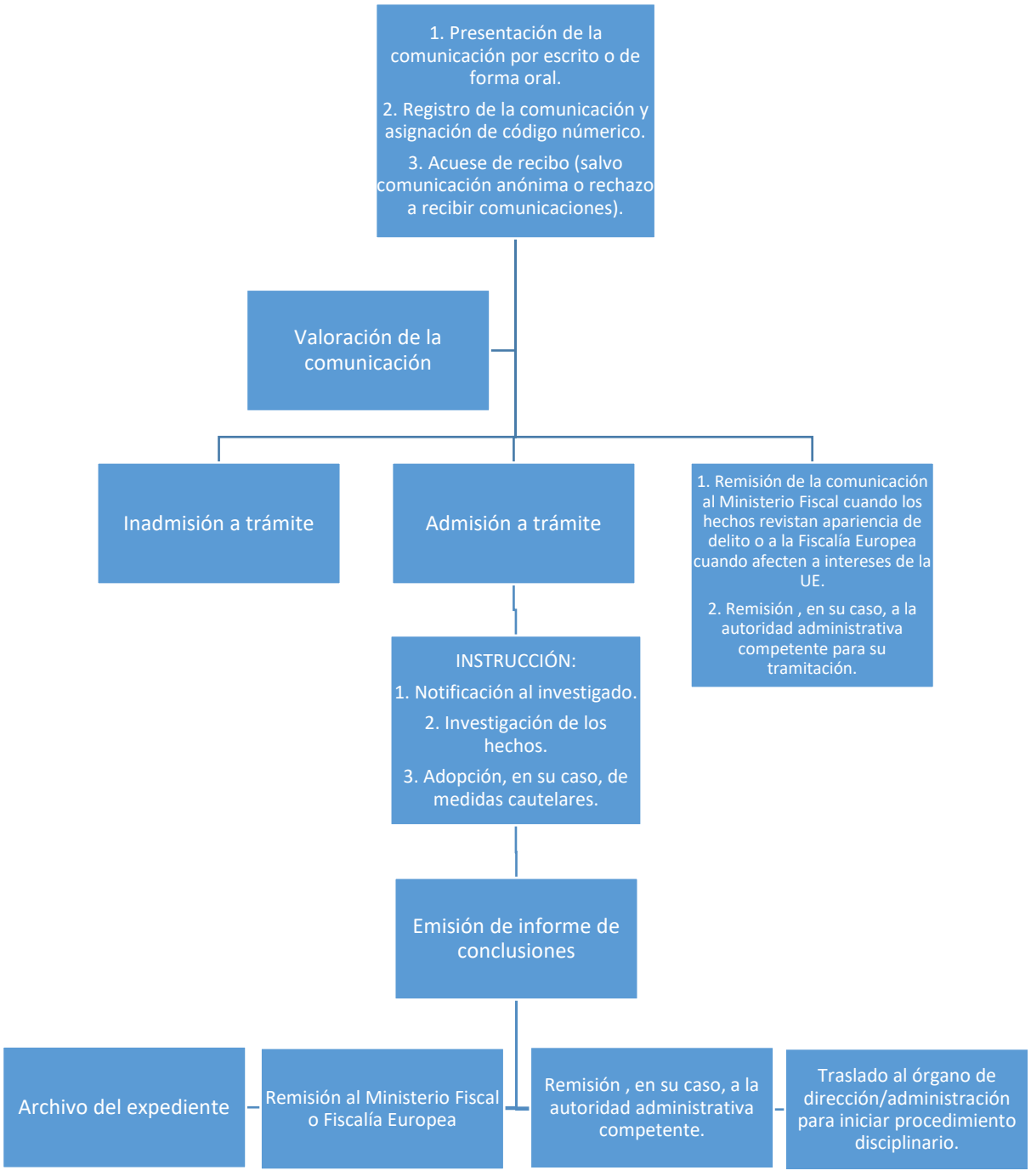
Una vez concluida la fase de instrucción, el Responsable del Sistema de Información elaborará un informe de conclusiones en el que se hará constar:

- Número de expediente y fecha.
- Relato de los hechos con los datos personales identificativos seudonimizados.
- Las actuaciones y pruebas realizadas para comprobar la verosimilitud de los hechos comunicados.
- Medidas cautelares que, en su caso, se hayan adoptado.
- Calificación y valoración de los hechos según las conclusiones alcanzadas en la instrucción.

A la vista de este informe de conclusiones el Responsable del Sistema Interno de Información adoptará alguna de las siguientes medidas:

1- Archivo del expediente cuando, de las investigaciones practicadas, los hechos no tengan apariencia de conducta irregular.
2- Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea u órgano competente.
3- Traslado de los hechos a la autoridad administrativa competente cuando se considere que esta debe iniciar un expediente administrativo sancionador.
4- Remisión al órgano de dirección y administración para la adopción de las medidas disciplinarias que pudieran corresponder por

vulneración de la política de la empresa, códigos de conducta, transgresión de la buena fe contractual, etc.



Si de la valoración de la instrucción se dedujere que la denuncia se ha presentado de mala fe, o que los datos o testimonios son falsos, el Responsable del Sistema Interno propondrá a la Dirección de la

empresa la incoación de correspondiente expediente disciplinario a las personas responsables de dichos comportamientos, sin perjuicio de otras responsabilidades en las que pueda incurrir según la legislación aplicable.

j) ¿Cuál es el plazo máximo para dar respuesta a las actuaciones de investigación?

No podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante (por tratarse de un informante anónimo o renuncia del derecho a recibir notificaciones), a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

k) Registro de informaciones

La persona designada como Responsable del Sistema Interno de Información deberá elaborar y custodiar un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la Ley.

Este registro no será público y únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con lo dispuesto en la ley. **En ningún caso podrán conservarse los datos por un período superior a diez años**.

l) Canal externo de información ante la Autoridad Independiente de Protección del Informante (A.A.I.).

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 prevé que cualquier persona 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 Autoridad Independiente de Protección del Informante es una autoridad administrativa independiente sometida al régimen jurídico de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Esta Autoridad Independiente de Protección del Informante constituye el canal externo a través del cual las personas informantes pueden comunicar las infracciones de las que tengan conocimiento. La misma tiene facultades de investigación y potestad sancionadora.

El procedimiento ante la Autoridad Independiente de Protección del Informante se encuentra regulado en el Título III de la Ley.

Toda persona física podrá informar ante la misma de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023, ya sea directamente o previa comunicación a través de este Canal interno de información.

Web: https://www.proteccioninformante.gob.es/

Email: canal.externo@proteccioninformante.es

Dirección postal: Autoridad Independiente de Protección del Informante, Calle Luis Cabrera 9, 28002 Madrid)

m) Otros canales externos.

Canales externos en la Unión Europea

Los informantes disponen de los siguientes canales externos para la comunicación de infracciones de las normas e intereses de la Unión Europea:

1. **Oficina Europea de Lucha contra el Fraude (OLAF):**

La OLAF dispone de un canal externo para la denuncia de fraudes u otras irregularidades graves con posibles repercusiones negativas para los fondos públicos de la UE (ingresos, gastos o activos de las instituciones de la UE).

Las denuncias pueden formularse de forma anónima a través de los siguientes medios:

- En línea, a través del Sistema de notificación de fraudes: https://fns.olaf.europa.eu/main_es.htm

- Por correo postal:
  European Commission
  European Anti-Fraud Office (OLAF)
  1049 Brussels
  Bélgica

2. Fiscalía Europea (EPPO):

La Fiscalía Europea es un órgano independiente de la Unión Europea encargado de investigar los delitos que atenten contra los intereses financieros de la UE y de ejercer la acción penal contra sus autores y llevarlos a juicio, en particular en lo que respecta al fraude, la corrupción, blanqueo de dinero y fraude transfronterizo en materia de IVA.

Las denuncias pueden formularse:

- En línea, a través del servicio «Report a Crime»:

  https://www.eppo.europa.eu/es/form/eppo-report-a-crime

  La Fiscalía Europea no recibe denuncias anónimas, por lo que la comunicación de infracciones a través de este canal requiere la identificación previa del informante.

Otros canales externos a nivel nacional

1. Servicio Nacional de Coordinación Antifraude (SNCA)

El SNCA es el órgano encargado de coordinar las acciones encaminadas a proteger los intereses financieros de la Unión Europea contra el fraude, en colaboración con la Oficina Europea de Lucha contra el Fraude (OLAF). A través del canal de denuncias habilitado, pueden reportarse informaciones sobre fraudes o irregularidades que afecten a fondos europeos.

Las denuncias pueden formularse en línea, a través del servicio Infofraude:

https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/Paginas/denan.aspx

El formulario del SNCA no permite denuncias anónimas, por lo que la comunicación de infracciones a través de este canal requiere la identificación previa del informante.

Adicionalmente, el SNCA ha habilitado un correo electrónico a través del cual se pueden plantear dudas y preguntas:
consultasantifraude@igae.hacienda.gob.es

Canales externos de ámbito autonómico

Para la comunicación de incumplimientos que se circunscriban a su ámbito territorial y que no sean competencia de la Autoridad Independiente de Protección al Informante, algunas comunidades autónomas han habilitado canales externos de información propios.

Hasta el momento se han constituido:

1. Oficina Antifraude de Cataluña (OAC).
   https://www.antifrau.cat/es
   https://seuelectronica.antifrau.cat/es/
2. Oficina Andaluza Antifraude (OAAF).
   https://antifraudeandalucia.es/
   https://antifraudeandalucia.sedelectronica.es/catalog/t/2c66e618-ffe7-4a1b-a14e-d55f26f9aa36
3. Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears (OAIB).
   https://www.oaib.es/
   https://oaib.sedelectronica.es/dossier.1
4. Agencia Antifraude de la Comunidad Valenciana.
   https://www.antifraucv.es/
   https://sede.antifraucv.es/carpetaciudadana/tramite.aspx?idtramite=16811
5. Oficina de Buenas Prácticas y Anticorrupción de la Comunidad Foral de Navarra (OANA).
   https://oana.es/es
   https://oana.sedelectronica.es/dossier.1

n) Protección de datos de carácter personal.

Los tratamientos de datos personales que se deriven de la tramitación del presente procedimiento de gestión de informaciones se realizarán de conformidad con lo dispuesto en el Titulo VI de la Ley 2/2023.

El Sistema interno de información impide el acceso no autorizado y preserva la identidad y garantiza la confidencialidad de los datos

correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

Así pues, la identidad del informante será en todo caso reservada, no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

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, y estos casos estarán sujetos a las salvaguardas establecidas en la normativa aplicable.

Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

El acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos.

Si la información recibida contuviera categorías especiales de datos, se procederá a su inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial conforme a lo

previsto en el artículo 9.2.g) del Reglamento general de protección de datos, según dispone el artículo 30.5 de la Ley 2/ 2023.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

En todo caso, transcurridos 3 meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

A continuación se facilita la información sobre el tratamiento de datos personales en el marco del Sistema de información.

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES

1. ***¿Quién es el responsable del tratamiento de sus datos?***

EXPORTADORA DATA BASE S.A.
C/DOÑANA 1 28924 ALCORCON (MADRID)
916104572
administracion@edb.es

2. ***¿Con qué finalidad tratamos sus datos personales?***
Sus datos serán tratados con la finalidad de gestionar el Sistema Interno de Información y Defensa del Informante 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, en este sentido, se tratarán para:

- *Gestionar, tramitar e investigar las comunicaciones presentadas a través del citado canal.*
- *Garantizar la confidencialidad, integridad y disponibilidad del sistema, así como la protección de las personas informantes frente a represalias.*
- *Cumplir con las obligaciones legales de la organización en materia de prevención y detección de irregularidades.*

3. ***¿Cuál es la legitimación para el tratamiento de sus datos?***
Le indicamos que la base legal para el tratamiento de sus datos es:

- *El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, artículo 6.1 letra c) del RGPD, en los supuestos de comunicación internos, cuando sea obligatorio disponer de un sistema interno de información.*

- *Si no fuese obligatorio, el tratamiento se presumirá lícito por ser necesario para el cumplimiento de una misión realizada en interés público el artículo 6.1.e) del RGPD.*

- *El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g)*

- *Consentimiento expreso del informante para documentar las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz. La conservación y registro de las denuncias realizadas a través de línea telefónica y sistemas de mensajería de voz con grabación, así como para la grabación de la reunión personal solicitada con la entidad con la finalidad de denunciar (Artículo 7 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.).*

4. ¿Por cuánto tiempo conservaremos sus datos?

Los datos se conservarán durante el tiempo necesario para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados, y, en su caso, mientras se tramiten las investigaciones y procedimientos derivados, no excediendo los plazos establecidos legalmente. En este sentido, se conservarán los datos de conformidad con lo previsto por el art. 32 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de la lucha contra la corrupción y normativa de aplicación.

Si se acreditara que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

5. ¿A qué destinatarios se comunicarán sus datos?

No se cederán datos a terceros, salvo obligación legal.

La identidad de los informantes o de quienes lleven a cabo una revelación pública, en ningún caso será comunicada a las personas a las que se refieren los hechos relatados ni a terceros. Así pues, la persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

El acceso a los datos se limitará exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen, para lo cual, como el resto de encargados de tratamiento, tenemos formalizado el contrato que regula dicho tratamiento de datos que exige la legislación vigente en materia de protección de datos personales.

e) El delegado de protección de datos.

En este sentido, será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan. Los datos personales generados por esta actividad de tratamiento, pueden ser comunicados, en su caso, al Ministerio Fiscal, los órganos jurisdiccionales y/o a las Fuerzas y Cuerpos de Seguridad del Estado y autoridad administrativa competente en el marco de la investigación penal, disciplinaria o sancionadora. El personal con funciones de gestión y control de recursos humanos sólo podrá acceder a dichos datos en caso de procedimientos disciplinarios contra una persona trabajadora, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo.

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países, en caso de que se produjeran, se informará debidamente y se garantizarán mediante mecanismos adecuados conforme al capítulo V del RGPD.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en la empresa estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos.

En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. En este caso, el responsable del tratamiento dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Podrá ejercitar materialmente sus derechos de la siguiente forma: dirigiéndose a la dirección de correo indicada en el primer apartado relativo a los datos del responsable del tratamiento. Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.aepd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en la empresa proceden del propio interesado, del informante o de terceros en el marco de las investigaciones llevadas a cabo.

9. Categoría de datos objeto de tratamiento

Podrán tratarse datos de carácter identificativo y de contacto del informante, en su caso, personas afectadas o terceros, datos profesionales o laborales, datos económicos o financieros relacionados con los hechos denunciados, datos incluidos en la comunicación o aportados en el curso de la investigación. Los datos pertenecientes a categorías especiales de datos sólo cuando sean estrictamente necesarios conforme al art. 30.5 de

la Ley 2/2023, de 20 de febrero y al art. 9.2.g del RGPD, en caso contrario, serán inmediatamente suprimidos. En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2 de la Ley 2/2023, de 20 de febrero, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley 2/2023, de 20 de febrero.

ANEXO 1

MODELO COMUNICACIÓN DE INFORMACIÓN (DENUNCIA) ANTE EL RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

*** Es posible informar de forma anónima, en cuyo caso no rellene los datos correspondientes al informante.**
**** La identidad del informante será en todo caso reservada y no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.**
***** TIENE LA POSIBILIDAD DE PRESENTAR SU COMUNICACIÓN ANTE LA AUTORIDAD INDEPENDIENTE DE PROTECCIÓN DEL INFORMANTE (A.A.I.) y otros canales externos**

Informante/denunciante (**si no es anónima**)	Persona/s denunciada/s (afectada/s)
Nombre y apellidos: Departamento o área al que pertenece: Email o dirección postal (si desea recibir notificaciones):	Nombre y apellidos: Departamento o área al que pertenece:

Fecha de los hechos:

DESCRIPCIÓN DE LOS HECHOS DENUNCIADOS:

PRUEBAS QUE APORTA:

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES

1. **¿Quién es el responsable del tratamiento de sus datos?**

   EXPORTADORA DATA BASE S.A.
   C/DOÑANA 1 28924 ALCORCON (MADRID)
   916104572

administracion@edb.es

2. **¿Con qué finalidad tratamos sus datos personales?**
   Sus datos serán tratados con la finalidad de gestionar el Sistema Interno de Información y Defensa del Informante 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, en este sentido, se tratarán para:

- Gestionar, tramitar e investigar las comunicaciones presentadas a través del citado canal.
- Garantizar la confidencialidad, integridad y disponibilidad del sistema, así como la protección de las personas informantes frente a represalias.
- Cumplir con las obligaciones legales de la organización en materia de prevención y detección de irregularidades.

3. **¿Cuál es la legitimación para el tratamiento de sus datos?**
   Le indicamos que la base legal para el tratamiento de sus datos es:

- El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, artículo 6.1 letra c) del RGPD, en los supuestos de comunicación internos, cuando sea obligatorio disponer de un sistema interno de información.

- Si no fuese obligatorio, el tratamiento se presumirá lícito por ser necesario para el cumplimiento de una misión realizada en interés público el artículo 6.1.e) del RGPD.

- El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g)

- Consentimiento expreso del informante para documentar las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz. La conservación y registro de las denuncias realizadas a través de línea telefónica y sistemas de mensajería de voz con grabación, así como para la grabación de la reunión personal solicitada con la entidad con la finalidad de denunciar (Artículo 7 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.).

4. **¿Por cuánto tiempo conservaremos sus datos?**

   Los datos se conservarán durante el tiempo necesario para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados, y, en su caso, mientras se tramiten las investigaciones y procedimientos derivados, no excediendo los plazos establecidos legalmente. En este sentido, se conservarán los datos de conformidad con lo previsto por el art. 32 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de la lucha contra la corrupción y normativa de aplicación.

   Si se acreditara que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

   En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

5. **¿A qué destinatarios se comunicarán sus datos?**

No se cederán datos a terceros, salvo obligación legal.

La identidad de los informantes o de quienes lleven a cabo una revelación pública, en ningún caso será comunicada a las personas a las que se refieren los hechos relatados ni a terceros. Así pues, la persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

El acceso a los datos se limitará exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen, para lo cual, como el resto de encargados de tratamiento, tenemos formalizado el contrato que regula dicho tratamiento de datos que exige la legislación vigente en materia de protección de datos personales.

e) El delegado de protección de datos.

En este sentido, será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan. Los datos personales generados por esta actividad de tratamiento, pueden ser comunicados, en su caso, al Ministerio Fiscal, los órganos jurisdiccionales y/o a las Fuerzas y Cuerpos de Seguridad del Estado y autoridad administrativa competente en el marco de la investigación penal, disciplinaria o sancionadora. El personal con funciones de gestión y control de recursos humanos sólo podrá acceder a dichos datos en caso de procedimientos disciplinarios contra una persona trabajadora, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo.

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países, en caso de que se produjeran, se informará debidamente y se garantizarán mediante mecanismos adecuados conforme al capítulo V del RGPD.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en la empresa estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos.

En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. En este caso, el responsable del tratamiento dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Podrá ejercitar materialmente sus derechos de la siguiente forma: dirigiéndose a la dirección de correo indicada en el primer apartado relativo a los datos del responsable del tratamiento. Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.aepd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en la empresa proceden del propio interesado, del informante o de terceros en el marco de las investigaciones llevadas a cabo.

9. Categoría de datos objeto de tratamiento

Podrán tratarse datos de carácter identificativo y de contacto del informante, en su caso, personas afectadas o terceros, datos profesionales o laborales, datos económicos o financieros relacionados con los hechos denunciados, datos incluidos en la comunicación o aportados en el curso de la investigación. Los datos pertenecientes a categorías especiales de datos sólo cuando sean estrictamente necesarios conforme al art. 30.5 de la Ley 2/2023, de 20 de febrero y al art. 9.2.g del RGPD, en caso contrario, serán inmediatamente suprimidos. En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2 de la Ley 2/2023, de 20 de febrero, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley 2/2023, de 20 de febrero.