CANAL DE DENUNCIAS DEL COMGI

INFORMACIÓN PREVIA AL USO DEL CANAL DE DENUNCIAS.

La Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, indica en su preámbulo que la colaboración ciudadana resulta indispensable para la eficacia del Derecho. Tal colaboración no sólo se manifiesta en el correcto cumplimiento personal de las obligaciones que a cada uno corresponden, sino que también se extiende al compromiso colectivo con el buen funcionamiento de las instituciones públicas y privadas. Dicha colaboración ciudadana es un elemento clave en nuestro Estado de Derecho.

Y seguidamente añade: *"No obstante, también ha de advertirse que, en ocasiones, esos loables comportamientos cívicos han generado consecuencias penosas para quienes han comunicado tales prácticas corruptas y otras infracciones, como son las presiones por parte de los denunciados, por lo que resulta indispensable que el ordenamiento jurídico proteja a la ciudadanía cuando muestra una conducta valiente de clara utilidad pública."*

Consecuentemente con ello la finalidad de la norma es proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos que la propia Ley regula; y engloba en su ámbito tanto las infracciones del derecho de la Unión, previstas en la Directiva citada, como las infracciones penales y administrativas graves y muy graves del ordenamiento jurídico español, ampliando de ese modo el ámbito material de la Directiva.

Por otra parte, la buena fe, es decir la conciencia honesta de que se han producido o pueden producirse hechos graves perjudiciales constituye un requisito indispensable para la protección del informante, excluyéndose, por lo tanto, otras actuaciones como la remisión de informaciones falsas o tergiversadas, así como aquellas que se han obtenido de manera ilícita.

En cuanto a las personas protegidas por la norma frente a posibles represalias, se extiende a todas aquellas personas que tienen vínculos profesionales o laborales con entidades tanto del sector público como del sector privado e incluso a las que ya hayan finalizado su relación o participan en procesos de selección, incluyendo también a las personas que prestan asistencia a los propios informantes.

El régimen jurídico del Sistema Interno de Información está constituido tanto por el "canal", entendido como buzón o cauce para recepción de la información, como al Responsable del Sistema y el propio procedimiento.

El sistema ha de permitir y permite la comunicación anónima; es más la Directiva establece como principio general el deber de mantener al informante en el anonimato. Sin embargo, y como es lógico, este pilar se exceptúa cuando o bien la norma nacional prevé revelarlo, o bien se solicita en el marco de un proceso judicial, lo que puede ocurrir por la decisión del juzgador de conocer la identidad de quien denunció, para garantizar el derecho de defensa del denunciado.

Este canal interno permite realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo electrónico o postal, o a través de cualquier medio electrónico habilitado al efecto, 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.

La Ley prevé que se advierta al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (de protección de datos).

Quienes realicen la comunicación a través de canales internos serán informados, de la existencia canales externos de información ante las autoridades competentes.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las comunicaciones.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante el sistema de mensajería de voz, de documentarán de alguna de las maneras siguientes, previo consentimiento del informante:

a) mediante una grabación de la conversación

b) mediante una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. En este caso se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar la transcripción.

¿QUIENES PUEDEN USAR ESTE CANAL?

Todas las personas referidas en el artículo 3 Es decir, aquellas 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 del COMGI, incluidos los miembros no ejecutivos.

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

El informante debe ser siempre de buena fe. 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.

¿DE QUÉ SE PUEDE INFORMAR A TRAVÉS DEL CANAL?

Se puede comunicar información sobre las infracciones previstas en el artículo 2 de la ley, es decir:

a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

1.ª Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;

2.ª Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o

3.ª Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

b) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES:

1. Identificación del canal interno de información: El canal interno de información del COMGI se articula mediante la aplicación informática de código abierto GLOBALLEAKS.

Se trata de una aplicación open-source software, es decir de código abierto lo que permite la mayor transparencia posible en materia informática y a través de la cual cualquier persona puede formular una iniciativa de información de modo anónimo y seguro. La plataforma es usada en más de 10.000 proyectos en todo el mundo, incluyendo medios independientes, agencias públicas, corporaciones... Cumple también la norma IS0 37002, estándar global publicado para ayudar a implementar y mejorar sus canales de denuncias internos.

2. Información sobre los canales externos de información ante autoridades competentes:

3. Se enviará acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

4. El plazo máximo para dar respuesta a las actuaciones de investigación, será de tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, 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.

5. Dentro del procedimiento se prevé expresamente de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, solicitar a la persona informante algún tipo de información adicional.

6. Se garantiza el derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

7. Se garantiza la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, A tal efecto dicho personal ha sido formado en esta materia y advertido de la tipificación como

infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.

8. En todo el proceso se respetará escrupulosamente el derecho a la presunción de inocencia y al honor de las personas afectadas.

PROTECCION DE DATOS PERSONALES.

Se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y en el presente título.

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.

Licitud de los tratamientos de datos personales.

1. Se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de la ley 2/2023, a que se refiere el presente procedimiento.

2. El tratamiento de datos personales, en los supuestos de comunicación internos, se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información. Si no fuese obligatorio, el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento.

3. El tratamiento de datos personales en los supuestos de canales de comunicación externos se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

4. El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

5. 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) del Reglamento (UE) 2016/679.

Información sobre protección de datos personales y ejercicio de derechos.

1. Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018,de 5 de diciembre.

A los informantes y a quienes lleven a cabo una revelación pública se les informa, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

Se les comunica también que 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. (Arts. 26 y 33 de la ley 2/2023).

2. 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.

3. 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.

4. 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.

Tratamiento de datos personales en el Sistema interno de información.

1. 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.

2. 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.

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, 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.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

3. Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse 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.

4. 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. Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información a que se refiere el presente artículo.

Preservación de la identidad del informante y de las personas afectadas.

1. Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

2. Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar 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.

3. 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.

Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.