Claves de la nueva Ley de Protección del Informante

Corporate Compliance

El pasado 21 de febrero, ha sido publicado en el Boletín Oficial del Estado 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. Con ella se traspone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019, conocida como *"Directiva Whistleblowing".*

La entrada en vigor de la Ley se producirá el día 13 de marzo y **las empresas dispondrán de tres meses** desde su entrada en **vigor para adaptar sus sistemas a la nueva regulación o proceder a su implementación**, esto es hasta el **13 de junio de 2023.** Como excepción, **las empresas con menos de 249 trabajadores disponen** de plazo hasta el **1 de diciembre de 2023.**

La norma obliga a las empresas con 50 o más trabajadores a contar con un sistema interno de información (anteriormente denominados como canales de denuncias), así como con un sistema de gestión y protección de los informantes, evitando represalias contra ellos.

Desde Marimón Abogados hemos analizado el texto definitivo de la Ley para responder a los aspectos esenciales y más importantes que afectan a las organizaciones del sector privado de cara a una mejor comprensión de sus apartados, si bien alcance de Ley también incluye a las Administraciones Públicas.

Para cualquier información sobre el contenido de esta publicación:

Lucía Oliveró | **Responsable del área Corporate Compliance**
lolivero@marimon-abogados.com

Anahita Tárrega | **Socia**
tarrega@marimon-abogados.com

¿Cuál es la finalidad de la Ley?

La protección frente a las represalias que pueden sufrir las personas físicas que informen sobre determinadas infracciones dentro de su ámbito laboral o profesional a través de los procedimientos de comunicación que están previstos en la Ley.

¿Qué procedimientos de comunicación están previstos por la Ley?

La Ley implica el establecimiento de dos sistemas de información que puedan garantizar la confidencialidad del informador: (i) **un canal interno** que esté instaurado dentro de las organizaciones y; (ii) **otro canal externo** que estará gestionado por la **Autoridad Independiente de Protección del Informante (AAI)**[1].

Toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante AAI), de la comisión de cualesquiera acciones u omisiones, ya sea directamente o previa comunicación a través del correspondiente canal interno.

¿Quién está obligado a cumplir con la Ley?

a) En el **sector privado**: (i) empresas a partir de 50 empleados; (ii) todas las empresas en el ámbito de aplicación de los actos de la Unión Europea y; (iii) partidos políticos, sindicatos, patronales y fundaciones.
b) En el **sector público**: (i) Administración General del Estado, administraciones regionales y provinciales; (ii) organismos y entidades públicas vinculadas o dependientes de alguna Administración Pública; (iii) corporaciones de Derecho Público; (iv) universidades públicas; (v) las autoridades administrativas independientes, el Banco de España y las entidades gestoras y servicios comunes de la Seguridad Social y; (vi) las fundaciones del sector público.

[1] En el plazo de un año desde la entrada en vigor de la Ley, el Consejo de Ministros aprobará mediante real decreto, a propuesta conjunta de los Ministerios de Justicia y de Hacienda y Función Pública, el Estatuto de la Autoridad Independiente de Protección del Informante (AAI) en el que se establecerán las disposiciones oportunas sobre organización, estructura, funcionamiento, así como todos los aspectos que sean necesarios para el cumplimiento de las funciones asignadas.

¿Sobre qué cuestiones se podrá informar a través del canal?

- **Acciones u omisiones** que puedan constituir **infracciones del Derecho de la Unión Europea**[2];
- **Acciones u omisiones** que puedan **ser constitutivas de infracción penal o administrativa grave o muy graves.**

Para que la información o comunicación pueda ser objeto de especial protección, **se tiene que haber realizado con buena fe**; deben **existir motivos razonables de veracidad de la** posible **infracción; y** debe **encontrarse dentro del ámbito de protección de la Ley**.

¿A quién protege la Ley?

La Ley recoge una nueva nomenclatura para el conocido como "denunciante" que pasa a denominarse "informante".

La Ley protege a los **informantes** que **trabajen en el sector privado o público** y que **hayan obtenido información sobre infracciones en un contexto laboral o profesional**: (i) trabajadores por cuenta ajena; (ii) autónomos; (iii) accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa; (iv) plantilla de contratistas, subcontratistas y proveedores; e incluso (vi) voluntarios, becarios y trabajadores en periodos de formación con o sin retribución.

Medidas de protección del informante

El informante estará protegido frente a las medidas que pudieran adoptarse como represalia, durante el plazo de dos años.

Cuando el **informante haya demostrado que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia**, y **corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos justificados** ajenos a la comunicación. Los **actos constitutivos de represalia serán nulos** y darán lugar a medidas disciplinarias, incluyendo una indemnización de daños y perjuicios.

[2] Quedan incluidos los siguientes sectores: contratación pública, servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, seguridad de productos y conformidad, seguridad del transporte, protección del medio ambiente y clima, protección frente a las radiaciones y seguridad nuclear, seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, salud pública, protección de los consumidores, protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

¿Qué requisitos deben cumplir los sistemas de información internos?

Nos centraremos en ver como se regulan **los canales de denuncia en las empresas del sector privado**, que ahora pasan a llamarse **Sistemas Internos de Información**.

- El **Órgano de Administración** de la empresa será el responsable de la implantación del sistema, **previa consulta a la representación legal de los trabajadores** y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.
- **Garantizar la confidencialidad** de la identidad del informante y de terceros y de las actuaciones que se desarrollen en la gestión y tramitación de la misma.
- Permitir **comunicaciones por escrito o verbalmente**, o de ambos modos. Toda comunicación de información (denuncia) deberá ser documentada, incluida las que se realicen de forma verbal.
- **Integrar los distintos canales internos** de información que pudieran establecerse dentro **de la entidad** (tales como, por ejemplo, canales de prevención del acoso, de la prevención de delitos o infracciones del código ético, etc.);
- Permitir **comunicaciones anónimas**;
- Contar con un **Responsable del Sistema de información**;
- Contar con una **política** que **regule el funcionamiento** del sistema, la defensa del informante y se **publicite en el seno de la entidad.**
- En caso de tener la empresa **página web, el canal deberá aparecer en la página de inicio**, en sección separada fácilmente identificable.
- **Contar con un procedimiento de gestión de las comunicaciones recibidas** y;

¿Cómo se gestionarán las comunicaciones recibidas a través del sistema interno de información?

La Ley establece que se deberá **desarrollar un procedimiento de gestión de las comunicaciones, aprobado por el Órgano de Administración**. El **Responsable del Sistema responderá de su tramitación diligente.**

En particular, el procedimiento responderá al contenido mínimo y principios siguientes:

- **Identificación del canal o canales internos** de información a los que se asocian;
- A quienes realicen la comunicación a través de canales internos se les **informará, de forma clara y accesible, sobre los canales externos de información** ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea;

- Enviar un **acuse de recibo** de la comunicación al informante en el plazo de **7 días naturales** siguientes a su recepción;
- Prever la **posibilidad de mantener la comunicación con el informante y, solicitarle información adicional;**
- Garantizar **el derecho del informante** a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oído;
- **Respetar la presunción de inocencia;**
- Garantía de **confidencialidad;**
- Determinar la **duración máxima de la investigación**, que no podrá ser superior **a tres meses**, salvo casos de especial complejidad que podrá extenderse tres meses más; y
- **Remisión de la información al Ministerio Fiscal** con carácter inmediato cuando los hechos pudieran ser indiciariamente **constitutivos de delito.**

El Responsable del Sistema

El **Órgano de Administración** será el **competente para la designación del Responsable del Sistema** y de su destitución o cese.

Tanto el **nombramiento como el cese del Responsable de Sistema deberá ser notificado a la Autoridad Independiente de Protección del Informante** en el **plazo** de **diez días** hábiles.

El Responsable del Sistema será un alto directivo de la entidad. Cuando la dimensión de la entidad no justifique lo anterior, el cargo podrá ser desempeñado por una persona que tenga otras funciones, tratando de evitar posibles conflictos de interés. Podrá **asumir la función de Responsable del Sistema el "Compliance Officer"** o responsable de cumplimiento normativo.

¿Puede externalizarse la gestión del sistema de información interno a un tercero?

Sí, la Ley permite externalizar la gestión siempre que el **tercero ofrezca garantías de respeto de la independencia, la confidencialidad y la protección de datos.**

El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales.

Registro de las comunicaciones

Las entidades obligadas deberán contar con **un libro-registro de las comunicaciones recibidas y de las investigaciones** internas a que hayan dado lugar.

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.

Grupos de sociedades

En el caso de un grupo de empresas, **la sociedad dominante aprobará una política general relativa al Sistema interno** de y asegurará la aplicación de sus principios **en todas las entidades que lo integran, sin perjuicio de la autonomía e independencia de cada sociedad** que, en su caso, pueda establecer el respectivo sistema de gobierno corporativo o de gobernanza del grupo, y de las modificaciones o adaptaciones que resulten necesarias para el cumplimiento de la normativa aplicable en cada caso.

El **Responsable del Sistema podrá ser uno para todo el grupo**, o bien **uno para cada sociedad** integrante del mismo. Por su parte, el **Sistema interno de información podrá ser uno para todo el grupo.**

Será admisible el intercambio de información entre los diferentes Responsables del Sistema del grupo, si los hubiera, para la adecuada coordinación y el mejor desempeño de sus funciones.

La Ley no regula expresamente los casos de multinacionales con filiales en distintos países. No obstante lo anterior, cuando la presencia internacional se limite a países de la UE las empresas deberán asegurarse de cumplir la Directiva comunitaria UE 2019/1937, de 23 de octubre y las correspondientes normativas nacionales de transposición en cada país.

Protección de Datos

El tratamiento de los datos personales en los canales de información se considera lícito cuando sea obligatorio disponer del sistema de información al ser necesario para el cumplimiento de una obligación legal. El tratamiento también se presume válido cuando el sistema no sea obligatorio, pero voluntariamente se decida crear uno, al ser necesario para la satisfacción del interés público.

Régimen sancionador

La Ley establece un régimen sancionador propio. Regula sanciones a imponer a las personas físicas o empresas en caso de incumplir con las obligaciones en la gestión y tramitación de las denuncias. La Ley categoriza las infracciones en muy graves, graves y leves, y para cada caso determina un plazo de prescripción y sanciones.

La potestad sancionadora corresponde a la **Autoridad Independiente de Protección del Informante (AAI).**

Constituye **una infracción muy grave no tener implantado el sistema o adoptar represalias contra los informantes**, sancionable con multa de 30.001€ a 300.000€ para las personas físicas, y multa de entre 600.001€ y 1.000.000€ para las personas jurídicas.

Se podrán imponer asimismo sanciones accesorias como la amonestación, la prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo de hasta cuatro años, así como la prohibición de contratar con el sector público durante tres años.

Conclusiones

No cabe duda de que la publicación de esta Ley supone un nuevo hito a nivel de cumplimiento para todas aquellas empresas que cuenten con 50 o más empleados, las cuales además de cumplir con los requisitos exigidos, deberán fomentar la integración y colaboración entre los distintos canales internos con los que ya contaba la empresa, como pueden ser el canal de denuncias en materia de acoso, prevención del blanqueo de capitales y el de protección de datos de carácter personal.

En definitiva, los sistemas internos de comunicación obligarán a las empresas sujetas a la Ley a adaptar sus sistemas internos a la nueva regulación o a proceder a su implantación con el objetivo de mejorar la transparencia, fomentando la colaboración de los propios empleados en las tareas de prevención y descubrimiento de actuaciones irregulares en el seno de una organización.

Para cualquier información sobre el contenido de esta publicación contamos con un equipo multidisciplinar en materia laboral, protección de datos y Compliance a disposición para contestar a las cuestiones que pudieran surgir al respecto.

Contacte con nosotros también, si necesita disponer de este documento en otro idioma.

Barcelona

Aribau, 185

08021

Tel.: +34 934 157 575

Madrid

Paseo de Recoletos, 16

28001

Tel.: +34 913 100 456

Sevilla

Balbino Marrón, 3

Planta 4ª-10

(Edificio Viapol)

41018

Tel.: +34 954 657 896

www.marimon-abogados.com