26.11.2019 ES Diario Oficial de la Unión Europea L 305/17

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

BOE

LEGISLACIÓN CONSOLIDADA

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.

Jefatura del Estado
«BOE» núm. 44, de 21 de febrero de 2023
Referencia: BOE-A-2023-4513

SERVICIOS PARA LA PROTECCIÓN DE LAS PERSONAS INFORMANTES Y CANAL DE DENUNCIAS DE INFRACCIONES Y CORRUPCCIÓN.

Adecuación a las exigencias del RGPD y a la LOPDGDD, implantando medidas de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, según la Ley 2/2023 y el RGPD.

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

BASE NORMATIVA Y CONCEPTUAL.

Las organizaciones son responsables de sus tratamientos sobre los datos personales y más concretamente el representante legal debe demostrar su responsabilidad activa y asegurar que sus tratamientos cuentan con las garantías suficientes y se han implementado las medidas necesarias para garantizar con la diligencia debida el cumplimiento de la normativa aplicable en materia de protección de datos (RGPD / LOPDGDD).

En 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, se emplea el término «denunciantes», y en esta ley se ha optado por la denominación «informante» y asimismo, se ha optado por emplear los términos «informaciones» y «comunicaciones» indistintamente.

En la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, se señala que la finalidad de la norma es la de 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 regulados.

RESPONSABILIDAD EN LAS ORGANIZACIONES.

El RGPD exige el cumplimiento del principio de *Accountability* o *Responsabilidad Proactiva,* el cual establece una obligación activa y sistemática del cumplimiento de la normativa de protección de datos, a través de la implantación de medidas técnicas y organizativas apropiadas.

Según la LOPDGDD y el RGPD, las organizaciones están obligadas a cumplir la normativa de protección de datos de carácter personal, lo cual incluye tanto a sociedades mercantiles tanto pymes como grandes empresas, autónomos y organismos públicos.

Por lo que se refiere a su ámbito de aplicación, además de proteger a quienes informen sobre las infracciones del Derecho de la Unión previstas en la Directiva del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, la Ley 2/2023 abarca también las infracciones penales y administrativas graves y muy graves de nuestro ordenamiento jurídico.

El Legislador ha considerado necesario, por tanto, ampliar en la Ley 2/2023 el ámbito material de la Directiva a las infracciones del ordenamiento nacional, pero limitado a las penales y a las administrativas graves o muy graves para permitir que tanto los canales internos de información como los externos puedan concentrar su actividad investigadora en las vulneraciones que se considera que afectan con mayor impacto al conjunto de la sociedad.

El Sistema Interno de Información (SII) es el cauce preferente para informar sobre las acciones u omisiones previstas en la Ley 2/2023 en su Artículo 2, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

Las personas jurídicas obligadas por las disposiciones del presente título dispondrán de un Sistema interno de información (SII) en los términos establecidos, que tiene por finalidad otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el Artículo 2. Ámbito material de aplicación, de la Ley 2/2023, a través de los procedimientos previstos en la misma.

También tiene como propósito el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de la organización y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

ÁMBITO DE APLICACIÓN.

Todas las organizaciones están obligadas a las normas legales y reglamentarias, puesto que recogen y tratan datos de personas físicas, debiendo no solamente cumplir sino poder demostrar el cumplimiento del RGPD Y LOPDGDD, así como de la Directiva (UE) 2019/1937 y de la Ley 2/2023, en los casos previstos.

Se aplicará a los informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

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

b) los autónomos;

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

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

Para poder gestionar adecuadamente el Sistema Interno de Información (SII) es necesaria la gestión de datos personales, por lo que a estos efectos, se incorporarán a las correspondientes actividades de tratamiento de la organización y serán tratados con la finalidad específica de cada tratamiento, de conformidad, principalmente, con la regulación establecida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

OBLIGACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN, SII.

Están obligadas a disponer un Sistema interno de información en los términos previstos en la Ley 2/2023:

a) Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores.

b) Las personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la Unión Europea en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente a que se refieren las partes I.B y II del anexo de la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, deberán disponer de un Sistema interno de información que se regulará por su normativa específica con independencia del número de trabajadores con que cuenten. En estos casos, esta ley será de aplicación en lo no regulado por su normativa específica.

c) Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta anteriormente, podrán establecer su propio Sistema Interno de Información, que deberá cumplir, en todo caso, los requisitos previstos en la Ley 2/2023.

VENTAJAS DE NUESTRO SISTEMA INTERNO DE INFORMACIÓN, SII.

El Representante Legal o Administrador de la organización es responsable de la implantación del SII, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa RGPD y LOPDGDD sobre protección de datos personales.

El Sistema Interno de Información, SII, promovido por CONTROL ALT SUP, tiene las siguientes ventajas:

a) Permite a todas las personas referidas en el ámbito personal de aplicación comunicar información sobre las infracciones previstas en la Ley 2/2023.

b) Está diseñado, establecido y gestionado de una forma segura, de modo que se garantiza la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permite la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integra los distintos canales internos de información que pudieran establecerse dentro de la entidad.

e) Garantiza que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad.

f) Es independiente y aparece diferenciado respecto de los sistemas internos de información de otras entidades u organismos, pudiendo compartir entre sí el SII y los recursos destinados a la gestión y tramitación de las comunicaciones, tanto si la gestión se lleva a cabo por cualquiera de ellas como si se ha externalizado.

g) Cuenta con un responsable del SII en los términos previstos en el artículo 8 de la Ley 2/2023.

h) Cuenta con una estrategia que enuncia los principios generales en materia de SII y defensa del informante y que es debidamente publicitada en el seno de la entidad.

i) Cuenta con un procedimiento de gestión de las informaciones recibidas.

j) Establece las garantías para la protección de los informantes en el ámbito de la propia entidad, respetando, en todo caso, lo dispuesto en el Procedimiento de Gestión de Informaciones.

PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES.

El procedimiento que CONTROLALTSUP pone a disposición del Cliente, tiene las siguientes prestaciones:

1. RESPONSABILIDADES.

Establecimiento de funciones, roles y responsabilidades del SII en la organización.

2. PROCESOS Y PRICIPIOS.

Desarrollo de las previsiones necesarias para que el SII y los canales internos de información existentes cumplan con los requisitos que están establecidos en la Ley 2/2023.

El contenido mínimo para cumplir con dichos requisitos en cuanto a procesos y principios son los siguientes:

a) IDENTIFICACIÓN DE LOS CANALES INTERNOS DE INFORMACIÓN A LOS QUE SE ASOCIAN.

b) INCLUSIÓN DE INFORMACIÓN CLARA Y ACCESIBLE SOBRE LOS CANALES EXTERNOS DE INFORMACIÓN.

c) ENVÍO DE ACUSE DE RECIBO DE LA COMUNICACIÓN AL INFORMANTE.

d) DETERMINACIÓN DEL PLAZO MÁXIMO PARA DAR RESPUESTA A LAS ACTUACIONES DE INVESTIGACIÓN.

e) PREVISIÓN DE COMUNICACIÓN CON LA PERSONA INFORMANTE.

f) ESTABLECIMIENTO DEL DERECHO DE LA PERSONA AFECTADA.

g) REMISIÓN DE LA INFORMACIÓN AL MINISTERIO FISCAL.

MEDIDAS DE PROTECCIÓN.

Las personas que comuniquen o revelen infracciones previstas en el alcance del PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES tendrán derecho a protección, para lo cual se incluyen en el SII los elementos siguientes:

a) CONDICIONES DE PROTECCIÓN.

b) PROHIBICIÓN DE REPRESALIAS.

c) MEDIDAS DE APOYO.

d) MEDIDAS DE PROTECCIÓN FRENTE A REPRESALIAS.

e) SUPUESTOS DE EXENCIÓN Y ATENUACIÓN DE LA SANCIÓN.

f) AUTORIDADES COMPETENTES.

POLÍTICA DE PROTECCIÓN DE LAS PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN.

El servicio de PROTECCIÓN DE LAS PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN, según la Ley 2/2023, pone a disposición del Cliente una Política que posibilita los procesos relacionados con elementos como los siguientes:

- PROTECCIÓN DE DATOS PERSONALES.
- OPERATIVA DEL CANAL DE DENUNCIAS.
- ACCESO Y FUNCIONAMIENTO DEL CANAL.
- REGISTRO Y CLASIFICACIÓN DE LAS DENUNCIAS.
- ANÁLISIS PRELIMINAR DE LOS HECHOS DENUNCIADOS.
- COMPROBACIÓN DE LOS HECHOS DENUNCIADOS.
- RESOLUCIÓN DE LA DENUNCIA.
- CONSERVACIÓN DE LA INFORMACIÓN.
- DENUNCIAS PROCEDENTES DE PERSONAS AJENAS A LA ORGANIZACIÓN.

Cuando se implanta la Política, se disponen entre otras de las siguientes prestaciones:

- RESERVORIO DE INFORMACIÓN DOCUMENTADA EXCLUSIVO EN LA NUBE.
- CONTROL DE ACCESOS MEDIANTE USUARIO Y CONTRASEÑA.
- SISTEMA INTERNO DE INFORMACIÓN, SII.
- PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES.
- MEDIDAS DE PROTECCIÓN.
- FORMULARIO DE DENUNCIAS.
- FICHA DE TRATAMIENTO DEL CANAL DE DENUNCIAS.
- ACUSE DE RECIBO A LA PERSONA INFORMANTE.

DELEGADO DE PROTECCIÓN DE DATOS, DPD.

Para ciertos tratamientos, que entrañen graves riesgos para los derechos y libertades de las personas, será obligatoria la designación de un DPD ante la AEPD. Ejemplos de ello son las actividades públicas, las sanitarias, la enseñanza, los colegios profesionales, etc.

El DPD debe asesorar e informar a la organización sobre el cumplimiento de las exigencias del RGPD en su organización, siendo sujetos obligados los incluidos en el Artículo 34 de la LOPDGDD.

Las entidades públicas o aquéllas participadas o que realicen una función pública requieren de la designación de un DPD, y por otro lado en el Artículo 24 de la LOPDGDD se recoge expresamente la licitud del tratamiento de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas. Dicha licitud deberá estar verificada por el DPD o de otro modo ser eliminada de forma diligente.

El DPD promoverá el cumplimiento de la POLÍTICA DE PROTECCIÓN en base a los registros y evidencias objetivas que se encuentran documentadas en el SII, supervisando el tratamiento realizado por el responsable y, en su caso, encargados como un método básico que les va a permitir identificar la adecuación a los requisitos del RGPD, con el objeto de poder valorar los aspectos que deben tener en cuenta, como por ejemplo durante los procesos de análisis y resolución de denuncias, comunicaciones, ayuda en las tareas de supervisión de la responsabilidad activa.

Disponibilidad 24-365.

- El Cliente recibirá tendrá acceso continuado y disponibilidad interrumpida las 24 horas al día durante los 365 días del año, para demostración del cumplimiento de los requisitos específicos de su actividad, así como para la adecuación a las exigencias RGPD y LOPDGG.

- Se trata de una herramienta informatizada versátil, flexible y específica, que sirve para que el Cliente reciba un servicio personalizado.

- Consta entre otros de los siguientes elementos:

  • ACCESO REMOTO AL SISTEMA DESDE CUALQUIER DISPOSITIVO.
  • INFORMACIÓN TÉCNICA Y JURÍDICA.
  • PROCEDIMIENTOS ESPECÍFICOS.
  • PROCESOS DE SU ACTIVIDAD.
  • REGISTROS DE GESTIÓN.
  • REGISTROS PROPIOS Y EXTERNOS.
  • SEGURIDAD, INTEGRIDAD, DISPONIBILIDAD Y AUTENTICIDAD.
  • CONFIDENCIALIDAD MEDIANTE ACCESOS RESTRINGIDOS.
  • CERO PAPELES -TODO EN LA NUBE.

- El Cliente está en condiciones de demostrar su adecuación, una vez alcanzado el nivel de cumplimiento.

- La protección de datos y la responsabilidad activa, resultan de fácil acceso y localización, para cualquier cuestión interna o externa de la organización.

- A través de la plataforma tecnológica de CONTROLALTSUP, el Cliente puede integrar diferentes sistemas e implantar los modelos de gestión, ya que su diseño hace más eficaz el manejo de la información documentada, mejora la planificación y la comunicación y disminuye tiempos y costos de dedicación.

- La organización puede gestionar informáticamente todos los procesos, integrándolos y permitiendo administrar la gestión de la producción en cualquier tratamiento de datos personales.

Para saber más:

https://garanteprivacy.es/

https://controlaltsup.com/