

El responsable del tratamiento de los datos personales, de conformidad con lo dispuesto en el Reglamento General (UE) 2016/679, de protección de datos (RPGD), Ley Orgánica 3/2018, de protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, le informa:

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

ONTIME CORPORATE UNION, S.A., (en adelante, "ONTIME") es el responsable del tratamiento de los datos de carácter personal que se traten a través del canal de denuncia interno (en adelante, el "Canal").

2. ¿Para qué tratamos sus datos personales?

Sus datos personales son tratados por el ONTIME para gestionar y tramitar las denuncias presentadas a través del Canal de denuncias.

3. ¿Qué categorías de datos personales tratamos?

Las categorías de datos personales que tratamos de usted dependen de la condición que tenga en la denuncia presentada. A continuación, se identifican las categorías de datos tratados en función de los diferentes interesados:

- Denunciante: se tratarán datos personales facilitados en la denuncia que pueden ser, a modo ejemplificativos, de carácter identificativo, de circunstancias sociales, de empleo, y datos especialmente protegidos.
- Denunciado: se tratarán datos identificativos, de circunstancias sociales, de empleo y datos especialmente protegidos.
- Testigo: se tratarán datos identificativos.

4. ¿De qué fuentes obtenemos sus datos personales?

Los datos de los denunciantes se obtienen de la denuncia presentada en el Canal.

Los datos de los denunciados y testigos se obtienen de la denuncia presentada en el Canal. En el caso de los testigos también habrán podido ser obtenidos del proceso de investigación realizado por el ONTIME.

5. ¿Cuál es la legitimación para el tratamiento de sus datos personales?

Trataremos sus datos personales sobre la base legitimadora de la obligación legal (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 el caso de que se traten datos especialmente protegidos (como datos de salud, vida sexual, afiliación sindical, opiniones políticas, convicciones religiosas...) los mismos serán tratados además sobre la base de que el tratamiento de dichos datos personales resulta necesario para la formulación o defensa de reclamaciones por parte del ONTIME o de la entidad a la que pertenezca el denunciado.

6. ¿Quién podrá acceder a sus datos personales?

Sólo los responsables de la investigación tienen acceso directo a los datos personales del informe. Los datos personales pueden ser revelados a terceros, como las autoridades o los auditores externos, en caso de obligación legal o interés legítimo.

Las personas que pueden tener acceso son:

- El responsable del Sistema de denuncia.
- El Delegado de Protección de Datos (DPO).
- El responsable de Recursos Humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- El responsable de los servicios jurídicos de la empresa, si procediera la adopción de medidas legales.
- La empresa que facilita un software del canal (Encargada del tratamiento).

Cuando se informa desde un dispositivo conectado a una red pública o de trabajo, las páginas web visitadas quedan registradas en el historial del navegador y/o en el registro del sistema, lo que podría permitir su identificación en algunas circunstancias, por lo que se recomienda al denunciante que utilice una red privada y el navegador en modo incógnito.

Los prestadores de servicios jurídicos, de sistemas informáticos y herramientas tecnológicas podrán acceder a sus datos personales durante la prestación de dichos servicios, si bien, dicho tratamiento de datos se realizará siempre bajo las directrices del ONTIME y serán devueltos o debidamente destruidos a la finalización del servicio contratado.

7. ¿A qué terceros se cederán sus datos personales?

Asimismo, en caso de que la denuncia presentada finalice con el inicio de un procedimiento judicial, sus datos personales serán cedidos a los Jueces y Tribunales y a nuestra aseguradora.

Si durante el proceso de investigación resulta necesario recabar datos personales especialmente protegidos, los mismos se podrán ceder, sobre la base de que el tratamiento resulta necesario para la formulación o defensa de reclamaciones.

Del mismo modo, el ONTIME podrá cederlos a terceros implicados en la investigación, que pasarán a ser también responsables.

8. ¿Se realizan transferencias internacionales de mis datos personales?

No hay transferencia internacional de datos personales.

9. ¿Cuánto tiempo conservamos sus datos personales?

Los datos incorporados a las denuncias y los derivados del procedimiento de investigación se conservarán durante la tramitación del expediente y una vez finalizado este, durante el tiempo necesario para la realización de las auditorías sobre la correcta actividad del canal de denuncias. 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.

No obstante, en caso de que se deriven acciones disciplinarias, administrativas o judiciales, sus datos personales se conservarán hasta la adopción de las citadas medidas, así como durante el plazo de prescripción de las acciones que resulten de aplicación.

10. ¿Cuáles son sus derechos?

Le informamos que tiene los siguientes derechos:

- derecho de acceso a sus datos personales para saber cuáles están siendo objeto de tratamiento y las operaciones de tratamiento llevadas a cabo con ellos;
- derecho de rectificación de cualquier dato personal inexacto;
- derecho de supresión de sus datos personales, cuando esto sea posible;
- derecho a solicitar la limitación del tratamiento de sus datos personales cuando la exactitud, la legalidad o la necesidad del tratamiento de los datos resulte dudosa, en cuyo caso, podremos conservar los datos para el ejercicio o la defensa de reclamaciones.
- derecho de oposición al tratamiento de sus datos personales. El ONTIME dejará de tratar sus datos salvo que tenga un interés legítimo imperioso o para la formulación, el ejercicio o la defensa de reclamaciones.

Podrá ejercitar sus derechos en cualquier momento y de forma gratuita dirigiendo comunicación a privacidad@ontimelogistica.com, indicando el derecho que desea ejercitar y sus datos identificativos.

Asimismo, le informamos que el ONTIME cuenta con un Delegado de Protección de Datos designado, con quién se podrá poner en contacto a través de la dirección anteriormente indicada.

Por otra parte, le informamos que tiene derecho a presentar una reclamación ante la autoridad de control competente (www.aepd.es) si considera una infracción de la legislación en materia de protección de datos respecto al tratamiento de sus datos personales.

ONTIME respeta los derechos y libertades fundamentales de las personas, entre los que se encuentra, el derecho fundamental a la protección de datos de carácter personal. La privacidad de los interesados es un pilar básico para ONTIME, tratando sus datos personales con escrupuloso respeto a la legislación vigente en materia de protección de datos personales, privacidad y seguridad de dicha información, para ello, se han adoptado las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos personales facilitados, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos.

También se han adoptado las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

A modo de ejemplo pueden adoptarse medidas como: 1) limitar el acceso al contenido de las denuncias a los usuarios que lleven a cabo la investigación y relacionarlos en el documento de seguridad; 2) establecer un sistema de registro de accesos, aun cuando no corresponda aplicar las medidas de nivel alto; 3) firma de compromisos reforzados de confidencialidad con los usuarios autorizados, con especiales medidas disuasorias para el caso de vulnerarse el deber de secreto.