Riesgo y cumplimiento de Edenred

01/12/2023

PROCEDIMIENTO DEL CANAL DE DENUNCIA

SAFE CHANNEL

Este procedimiento detalla el proceso de gestión de las alertas de denuncias comunicadas a través del canal de denuncia interna del Grupo (en adelante, SAFE Channel) y relativas a cualquier acto indebido que infrinja los principios descritos en la Carta Ética de Edenred, el Código de Conducta (manual de Edenred para prevenir la corrupción) y, de forma más general, cualquier infracción de las leyes de la UE.

Este, muestra el compromiso del Grupo con el cumplimiento de la DIRECTIVA UE 2019/1937 relativa a la protección de las personas que denuncien infracciones del Derecho de la Unión (en adelante, Directiva Europea 2019/1937) y 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.

CONTENIDO DEL PROCEDIMIENTO

PARTE 1: MARCO NORMATIVO, ALCANCE Y CONTEXTO DEL PROCEDIMIENTO

I. Una Directiva europea que refuerza el marco general para proteger a las personas que presentan denuncias

En octubre de 2019, fue emitida una Directiva europea sobre la protección de las personas que denuncian infracciones del Derecho de la Unión con el fin de garantizar una protección a los denunciantes en la Unión Europea. La directiva dispone que "los Estados miembros velarán para que las entidades jurídicas de los sectores privado y público establezcan canales y procedimientos de denuncia interna y de seguimiento".

La Directiva regula los plazos y pasos para procesar una alerta y obliga a garantizar una protección a los denunciantes.

Esta Directiva europea debe transponerse en todos los países de la UE. Por ejemplo, en España, 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, destinada a mejorar la protección de los denunciantes" para transponer las disposiciones de la Directiva europea. Esta refuerza la protección de los denunciantes prohibiendo cualquier represalia o desventaja luego de una denuncia.

II. Alcance del procedimiento

Este procedimiento es aplicable a EDENRED ESPAÑA y tiene el objeto de proporcionar directrices detalladas para el uso del canal de denuncia, SAFE Channel, así como de establecer el procedimiento de comunicación de denuncias a través de los canales externos al SAFE Channel.

III. Contexto del procedimiento

Edenred se compromete a hacer todo lo que esté a su alcance para garantizar que sus actividades se realicen en pleno cumplimiento de la ley. La credibilidad de la imagen de marca del Grupo y la sostenibilidad de la empresa dependen de ello.

De conformidad con la Directiva Europea 2019/1937 y 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. Este sistema de gestión de alertas profesionales es ofrecido a todos los asociados de Edenred (personal, trabajadores temporales, becarios, aprendices y proveedores externos que trabajan con Edenred)así como a cualquier tercero interesado, con el fin de que puedan presentar denuncias sobre una situación que no cumpla con la Carta de Ética, el Código de Conducta (manual de Edenred para prevenir la corrupción) y, de forma más general, cualquier infracción de las leyes locales y de la UE.

Este sistema es complementario y no pretende sustituir al canal de comunicación interna tradicional, es decir, los canales jerárquicos como una conversación con el gerente o con una persona del departamento jurídico, de compliance o de gestión de recursos humanos responsables de tratar estas alertas. Si no considera adecuado utilizar la vía de comunicación interna tradicional, o si cree que su alerta no se está procesando de manera oportuna, puede utilizar esta plataforma puesta a su disposición.

El sistema no está previsto como un sistema de emergencia. En caso de peligro inminente, se deberá entrar en contacto con las autoridades correspondientes.

PARTE 2: PROPÓSITO DEL SAFE CHANNEL

I. ¿Qué es el SAFE Channel?

Como parte del Programa SAFE, se ofrece a todos los asociados de Edenred (empleados y proveedores) así como a cualquier tercero interesado, un canal de denuncia, el SAFE Channel.

El objetivo del SAFE Channel es recopilar alertas sobre las siguientes infracciones:

- Infracciones que entran en el ámbito de aplicación de los actos de la Unión (Art. 2, Directiva 2019/1937 relativa a la protección de las personas que denuncian infracciones del Derecho de la Unión,
- Actos de infracción del Código de Conducta, es decir, corrupción, tráfico de influencias, casos de fraude, robo o divulgación de información confidencial,
- Actos de blanqueo de capitales o financiación del terrorismo (Directiva 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo)
- Infracciones que afecten a los intereses financieros de la UE (Directiva 2019/1937 de acuerdo con el art. 325 TFUE)
- Prácticas anticompetitivas (Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, la Ley 15/2007, de 3 de julio, de Defensa de la Competencia y el Real Decreto 261/2008, de 22 de febrero, por el que se aprueba el Reglamento de Defensa de la Competencia),
- Infracciones relativas al mercado interior de la UE. Especialmente, en materia de competencia y ayudas otorgadas por los Estados e infracciones fiscales en materia de Impuesto de Sociedades (Directiva 2019/1937 de acuerdo con lo establecido en el art. 26 TFUE)
- Actos de discriminación y acoso (de acuerdo con el Código de Conducta y el Protocolo para la prevención y actuación frente al acoso laboral, sexual y el acoso por razón de sexo en Edenred España)
- Violaciones de los derechos humanos o de las libertades fundamentales
- Infracciones graves y manifiestas de un reglamento con respecto al derecho laboral, la salud o la seguridad de las personas,
- Casos de infracción de datos personales con riesgo de vulneración de derechos y libertades (Reglamento 2016/679 RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales),
- Acciones u omisiones constitutivas de infracción penal o administrativa grave o muy grave. Se entenderán como graves o muy graves aquellas infracciones penales o administrativas que impliquen un perjuicio económico para la Hacienda Pública o la Seguridad Social.

Las denuncias deben cumplir los siguientes requisitos:

- Deben ser realizadas por una persona física, sin compensación económica y de buena fe
- Si la información no fue obtenida como parte de una actividad profesional, debe ser obtenida personalmente por el denunciante
- La denuncia es realizada usando el canal de denuncia interna o, en su defecto, a través del canal jerárquico (como la conversación con el gerente o con una persona del departamento jurídico, de compliance o de gestión de recursos humanos)

Después de evaluar la materialidad de los hechos alegados en la denuncia y la exactitud de la información proporcionada, el gestor del caso decidirá si procede tramitar la alerta (véase II.3.). En este caso, y si él mismo no se encarga de la denuncia, puede designar a una o más personas externas (por ejemplo, un abogado, un analista forense), encargadas de la investigación, en función del lugar y de la naturaleza de la denuncia.

Se ha definido una organización que incluye gestores de casos, puntos de contacto locales y comités para abarcar todas las unidades de negocio al nivel adecuado. Las alertas locales serán manejadas por gestores de casos. En Edenred España, se gestionará a través de la persona que ocupe el rol de Data Privacy & Security Compliance Regional, con el apoyo de los controladores financieros regionales. Ninguna otra persona/departamento aparte de los indicados está autorizado a procesar una denuncia.

II. Riesgos para la persona denunciada

Se presume que la persona denunciada ha actuado de acuerdo con la Carta Ética de Edenred y las leyes y reglamentos hasta que las pruebas reunidas durante la investigación establezcan razonablemente que no fueron respetados. Si al finalizar la investigación se considera que se deben tomar medidas disciplinarias, estas pueden consistir en la imposición de sanciones a la persona denunciada de conformidad con el reglamento interno o, en el caso de considerar que la conducta realizada puede ser constitutiva de delito, podrá presentarse una denuncia ante los tribunales competentes.

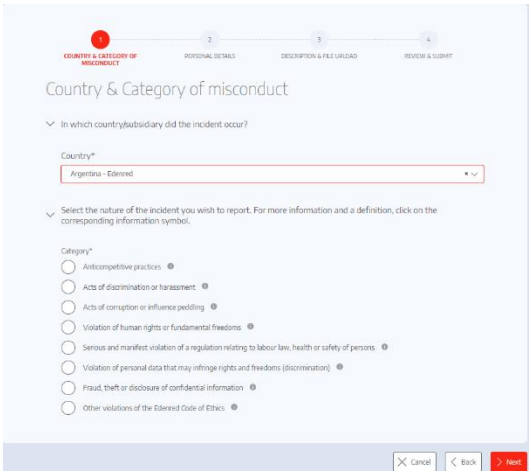
PARTE 3: CÓMO UTILIZAR EL SAFE CHANNEL

Para notificar una denuncia, la persona debe rellenar el formulario que figura en el enlace del SAFE Channel: https://edenred.integrityline.org/index.php.

I. Notificar una denuncia a través del canal de denuncia interna

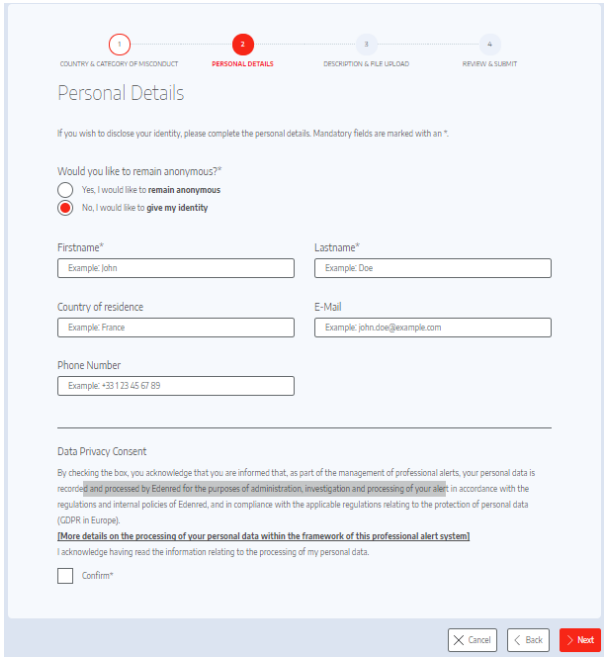
Para presentar una denuncia, el denunciante deberá seguir 4 pasos.

1- Completar la información sobre el país y la naturaleza del incidente:
   - País
   - La naturaleza del incidente (como se indica a continuación):



2- Completar los datos personales, en su caso, y dar su consentimiento para el procesamiento de datos personales

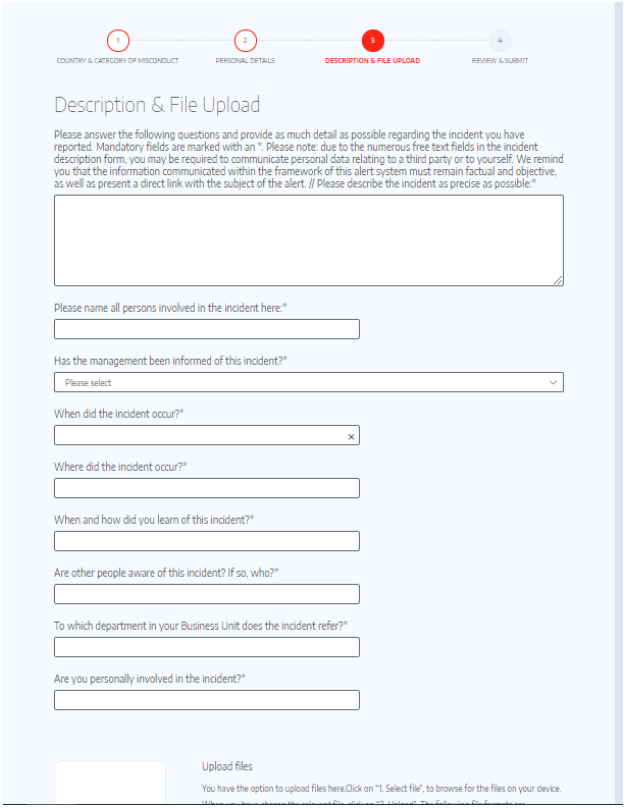
El denunciante podrá revelar su identidad o permanecer en el anonimato. La Directiva europea 2019/1937 y la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción garantizan la protección de la identidad de la persona que denuncia infracciones (véase Parte 4 -1 para obtener más información), ya sea que revele o no su identidad.


1
COUNTRY & CATEGORY OF MISCONDUCT
2
PERSONAL DETAILS
3
DESCRIPTION & FILE UPLOAD
4
REVIEW & SUBMIT
Personal Details
If you wish to disclose your identity, please complete the personal details. Mandatory fields are marked with an *.
Would you like to remain anonymous?*
Yes, I would like to remain anonymous
No, I would like to give my identity
Firstname*
Example: John
Lastname*
Example: Doe
Country of residence
Example: France
E-Mail
Example: john.doe@example.com
Phone Number
Example: +33 1 23 45 67 89
Data Privacy Consent
By checking the box, you acknowledge that you are informed that, as part of the management of professional alerts, your personal data is recorded and processed by Edenred for the purposes of administration, investigation and processing of your alert in accordance with the regulations and internal policies of Edenred, and in compliance with the applicable regulations relating to the protection of personal data (GDPR in Europe).
[More details on the processing of your personal data within the framework of this professional alert system]
I acknowledge having read the information relating to the processing of my personal data.
Confirm*
Cancel
Back
Next

3- Descripción y carga de archivos

La persona que notifica la denuncia debe indicar todos los detalles posibles y los hechos deben ser de seria gravedad para que el gestor del caso pueda procesar el asunto.

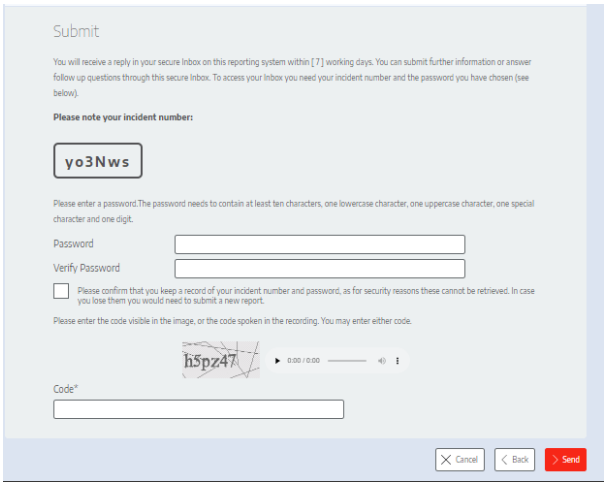
La redacción debe ser lo suficientemente objetiva y precisa para permitir la verificación de los presuntos hechos. Es importante ser preciso y proporcionar solo información directamente relacionada con el tema de la denuncia.



4- Revisar el informe y presentarlo

La última página permite al denunciante revisar la información antes de presentar la denuncia. El sistema genera un número de incidente y solicita crear una contraseña para acceder a la bandeja de entrada segura. El objetivo de la bandeja de entrada segura es crear un canal de comunicación entre el gestor del caso y el denunciante.

Cuando toda la información sea verificada y el número de incidente y contraseña estén guardados, se podrá enviar la denuncia.



II. Gestión del caso luego de su recepción

1- Acuse de recibo de la alerta

Después de recibir una alerta a través del canal de denuncia interna, el gestor del caso a cargo acusa recibo en un plazo de 7 días laborables a partir de su recepción enviando un correo electrónico en la bandeja de entrada segura al denunciante.

2- Evaluar si es necesario informar a la persona reportada

Las denuncias pueden mencionar a alguien por su nombre, y podría ser útil para el gestor del caso recopilar información de ese tercero. La información recopilada debe ser utilizada para investigar el caso y evaluar la autenticidad de los presuntos hechos.

La decisión de informar a la parte reportada debe ser tomada por el gestor del caso con la ayuda de la dirección local. Sin embargo, está prohibido revelar la identidad de la persona que presentó la denuncia o de las personas reportadas en la misma (véase Parte 4, para obtener más información)

De acuerdo con RGPD (Reglamento general de protección de datos) cuando se tratan datos de personas físicas, estas deberán ser informadas dentro del plazo de un mes, siempre que esto no ponga en riesgo las investigaciones en curso.

3- Condiciones para investigar el caso

El gestor del caso debe comprobar, a menos que la denuncia sea anónima, si esta cumple con las siguientes condiciones:

- Debe ser realizada por una persona física, sin compensación económica y de buena fe
- Si la información no fue obtenida como parte de una actividad profesional, debe ser obtenida personalmente por el denunciante
- La denuncia debe realizarse a través del canal de denuncia interna o, en su defecto, a través del canal jerárquico

➢ *El caso no cumple las condiciones anteriores:*

El gestor del caso podrá solicitar más información, si es necesario. Si la denuncia no cumple ninguna de las dos condiciones, el gestor del caso informará al denunciante de las razones por las cuales no se investigará el caso. La información debe ser enviada por correo electrónico utilizando la bandeja de entrada segura y cierra el informe.

➢ *El caso cumple con las condiciones:*

El gestor del caso debe proceder con el análisis de la denuncia.

4- Investigación del caso

El gestor del caso puede solicitar toda la documentación o información necesaria para evaluar la exactitud de la denuncia:

- ➢ *El denunciante no puede proporcionar más información:* el gestor del caso informa oportunamente del cierre del caso, utilizando la herramienta SAFE Channel porque la denuncia no es exacta o falta información
- ➢ *La información aportada en la denuncia no es concluyente:* el gestor del caso informa oportunamente del cierre del caso, utilizando la herramienta SAFE Channel porque los hechos no son exactos o no están fundamentados

- *La información aportada en la denuncia es concluyente:*
  - El gestor del caso convoca un Comité de Ética Regional e informa al Compliance Officer del Grupo
    - *Si el Comité de Ética considera que el caso no es concluyente:* el gestor del caso informa inmediatamente del cierre del caso, utilizando la herramienta SAFE Channel porque los hechos no son exactos o no están fundamentados
    - *Si el caso se considera concluyente:* el Comité de Ética informa al Gerente General y/o al equipo de RRHH para que tomen las medidas adecuadas e informa al denunciante de las medidas tomadas utilizando la herramienta SAFE Channel (véase el paso 5)

El gestor del caso debe informar al denunciante lo antes posible y, en todo caso, antes de **3 meses a partir de la fecha de la denuncia** (o del acuse de recibo de esta) de las medidas adoptadas o del cierre del caso.

En caso de que el denunciante no esté de acuerdo con las conclusiones, puede solicitar apelar o presentar el caso ante el Comité de Ética. El gestor del caso convoca un Comité de Ética de la Región e informa al Compliance Officer de Grupo (véase más arriba).

5- Adoptar las medidas adecuadas

Después o durante la reunión del Comité de Ética, el gestor del caso debe evaluar si es necesario adoptar sanciones disciplinarias.

- *Deben tomarse medidas disciplinarias:* Ponerse en contacto con el departamento local de RRHH para proceder a las sanciones
- *En caso contrario, el gestor del caso debe asegurarse de que no se anticipa ningún procedimiento judicial*
  - Si no es así, se deberá cerrar el caso y anonimizar los datos inmediatamente
  - En caso afirmativo, se deberá documentar el análisis y el gestor del caso deberá ponerse en contacto con la dirección local y los asesores jurídicos
    - En función del riesgo, se decidirá el periodo de conservación antes de anonimizar los datos y será necesario realizar un seguimiento anual.

III. Canal de denuncia externo a la plataforma SAFE Channel

La persona denunciante, podrá utilizar la plataforma SAFE para realizar la denuncia de forma externa a la herramienta SAFE Channel a través de las siguientes

1. Canal de denuncias Externo (Autoridad Independiente de Protección del denunciante)

El uso de un canal de denuncia interna no es obligatorio y el denunciante puede optar por denunciar un caso utilizando los canales de denuncia externa implementados a través de la Autoridad o Autoridades locales independientes. A estos efectos, en España, los organismos encargados de recoger estas denuncias son: para Cataluña, la Oficina Antifrau de Catalunya y para Madrid, la Oficina Municipal contra el Fraude y la Corrupción.

A efectos informativos, a través de los citados los canales externos, lo denunciantes pueden informar de casos en materia de:

- Infracciones que entran en el ámbito de aplicación de los actos de la Unión (Art. 2, Directiva 2019/1937 relativa a la protección de las personas que denuncian infracciones del Derecho de la Unión,

- Infracciones que afecten a los intereses financieros de la UE (Directiva 2019/1937 de acuerdo con el art. 325 TFUE)
- Infracciones relativas al mercado interior de la UE. Especialmente, en materia de competencia y ayudas otorgadas por los Estados e infracciones fiscales en materia de Impuesto de Sociedades (Directiva 2019/1937 de acuerdo con lo establecido en el art. 26 TFUE)
- Acciones u omisiones constitutivas de infracción penal o administrativa grave o muy grave. Se entenderán como graves o muy graves aquellas infracciones penales o administrativas que impliquen un quebranto económico para la Hacienda Pública o la Seguridad Social.

2. Comunicación por correo electrónico

El denunciante podrá, comunicar la denuncia directamente al Data Privacy & Security Compliance Regional a través del correo electrónico de uso exclusivo para este fin.

3. Comunicación por vía telefónica

El denunciante podrá, comunicar la denuncia directamente al Data Privacy & Security Compliance Regional a través del número telefónica de uso exclusivo para este fin.

4. Comunicación mediante reunión presencial

A solicitud del denunciante, también podrá presentar la denuncia mediante reunión presencial. Dicha solicitud podrá realizarse a través del correo electrónico o del número de teléfono habilitados y será atendida por el Data Privacy & Security Compliance Regional dentro del plazo máximo de siete días.

Las denuncias presentadas por un canal de Edenred externo a la plataforma SAFE Channel, se recibirán por el canal escogido por el denunciante, pero se introducirán en la herramienta SAFE Channel por parte del Data Privacy & Security Compliance Regional, para su inscripción, tramitación y gestión. A excepción de las comunicaciones dirigidas a agendar la reunión presencial, las comunicaciones con el denunciante que haya presentado la denuncia por un canal de Edenred externo a la plataforma SAFE Channel se realizarán a través de la herramienta.

PARTE 4: PROTECCIÓN DE LOS DENUNCIANTES Y DE LOS DATOS PERSONALES

I. Protección de los denunciantes

La Directiva europea 2019/1937 estableció un marco normativo armonizado en toda la UE para garantizar la protección de los denunciantes.

Por lo tanto, conforme al nuevo reglamento, un denunciante gozará de protección siempre que tenga motivos razonables para creer que la información revelada era verdadera en el momento de la denuncia. Una persona que haya denunciado una infracción de forma anónima pero que posteriormente sea identificada también gozará de la misma protección.

Por garantizar la protección, entendemos asegurar que la identidad del denunciante se mantenga confidencial y solo sea conocida por las personas que procesan la alerta. La identidad de la persona que informa de una infracción nunca se revelará a terceros, ni a la persona mencionada en una alerta, a menos que la ley obligue a hacerlo.

No se considerará que la comunicación constituye revelación de información ni el denunciante incurrirá en responsabilidad con la denuncia siempre que el denunciante la considere necesaria para revelar acción u omisión protegida por ley.

El denunciante tampoco incurrirá en responsabilidad respecto del modo de acceso a la información si dicho acceso no constituye delito.

En caso de que se abra un proceso judicial, incluidos los de difamación y revelación de secretos empresariales, los trabajadores no incurrirán en responsabilidad por ningún tipo de revelaciones en cumplimiento de la ley.

La duración de la protección será, como norma general, de 2 años una vez producida la revelación de la información. La autoridad competente, sin embargo, podrá ampliar dicho plazo de forma excepcional.

1. Prohibición de represalias

En Edenred, condenamos firmemente cualquier medida de represalia, o amenaza de represalia, tomada contra una persona que denuncie una infracción. Además, la Directiva Europea 2019/1937 obliga al Estado Miembro a implementar sanciones con el fin de evitar cualquier caso de represalia u obstrucción a una persona que denuncie un caso.

Se prohíbe cualquier tipo de represalia contra los denunciantes, específicamente:

- Suspensión del contrato de trabajo, despido o extinción de la relación laboral, terminación anticipada de un contrato o anulación de contrato de servicios, imposición de cualquier medida disciplinaria, no conversión de temporal a fijo, degradación o denegación de ascensos, etc.,
- Daños, incluidos de carácter reputacional, pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo,
- Evaluación o referencias negativas en el desempeño profesional,
- Inclusión en listas negras o difusión de información que dificulten o impidan al empleo o a la contratación de obras y servicios,
- Denegación o anulación de una licencia o permiso,
- Denegación de formación,
- Discriminación, o trato desfavorable o injusto.

En procedimientos de represalias ente un órgano jurisdiccional, se presumirá que el perjurio se ha sufrido por informar o por hacer una revelación pública.

II. Protección de datos

1. Datos personales

Como parte del proceso de envío de la alerta, el denunciante puede optar por permanecer en el anonimato o facilitar a Edenred sus datos personales, en particular: información sobre su identidad, nombre y apellido, país de residencia, número de teléfono y dirección de correo electrónico.

Dados los numerosos campos de texto libre del formulario de descripción de incidentes, el denunciante puede comunicar voluntariamente datos personales relativos a sí mismo o a un tercero. Cabe recordar que velaremos para que la información comunicada en el marco de este sistema de alerta se mantenga imparcial y objetiva y se refiera estrictamente al tema de la alerta. Las personas mencionadas en la alerta serán informadas – a su debido tiempo – de que son objeto de una alerta, de modo que tengan la oportunidad de presentar sus comentarios.

En todo caso, se preservará la confidencialidad del denunciante, las personas mencionadas en la alerta no recibirán ninguna información relativa a su identidad -en la medida de lo permitido por la ley- y su información se utilizará de forma que no se ponga en peligro su anonimato.

El tratamiento de sus datos personales en el marco de este sistema de alerta profesional es implementado para recopilar y procesar alertas destinadas a revelar un incumplimiento grave de un reglamento específico.

Por lo tanto, el tratamiento de las denuncias se basa en nuestra obligación legal de establecer un procedimiento adecuado para procesar dichas denuncias.

2. Propósito y base jurídica del tratamiento de datos personales

El tratamiento de los datos personales en el marco de este sistema de alerta profesional es implementado para recopilar y procesar denuncias destinadas a revelar un incumplimiento grave de un reglamento específico.

En relación con las denuncias por infracciones de la Carta Ética de Edenred, este tratamiento se basa para los Estados Miembros de la UE y los países en los que exista una Ley de Denuncia en el marco legal implementado por la Directiva Europea 2019/1937.

Para los demás países, el tratamiento se basa en los intereses legítimos que perseguimos, es decir, garantizar que nuestras actividades se realicen cumpliendo plenamente nuestras obligaciones legales y nuestras propias normas internas para proteger la confianza de nuestros clientes y socios, en particular: la protección de los activos de la empresa, la seguridad informática, la sinceridad y exactitud de la información comercial y financiera, la prevención del lavado de dinero, las relaciones con los proveedores, la lucha contra la discriminación, contra el trabajo forzado y encubierto y contra el trabajo infantil.

3. Conservación de los datos

Cuando consideramos que un informe no entra en el ámbito de este sistema de gestión de alertas profesionales, los datos se destruyen inmediatamente.

Cuando la denuncia entra en el ámbito del sistema, los datos personales se conservarán mientras dure la investigación y se eliminarán en un plazo de dos meses a partir del final de las operaciones de verificación. Si se abre un procedimiento disciplinario o contencioso, los datos personales se eliminarán al término de este, sujeto a la expiración de los medios y límites de tiempo para apelación sobre la posible infracción jurídica grave denunciada por la alerta:

- Para los actos de corrupción o tráfico de influencias, el plazo de prescripción es de 12 años a partir del día en que se cometió la infracción;
- En caso de fraude, robo o revelación de información confidencial, el plazo de prescripción es de 20 años a partir del día en que se cometió la infracción;

- En caso de infracción del Código Ético de Edenred, el plazo de prescripción es de 6 años a partir del día en que se cometió la infracción;
- Para las prácticas contrarias a la competencia, el plazo de prescripción es de 5 años a partir de la última investigación, hallazgo o sanción;
- Para los actos de discriminación o acoso, el plazo de prescripción es de 20 años a partir del día en que se cometió la infracción;
- Para una violación de los derechos humanos o las libertades fundamentales, el plazo de prescripción es de 30 años a partir del día en que se cometió la infracción;
- En caso de infracción grave y manifiesta de un reglamento en relación con el derecho laboral, la salud o la seguridad de las personas, el plazo de prescripción es de 2 años desde que se tuvo conocimiento de los hechos;
- En caso de infracción de datos personales que afecten los derechos y libertades de las personas, el plazo de prescripción es de 6 años a partir del día en que se cometió la infracción.

4. Derechos sobre los datos

Los denunciantes tienen derecho de acceso, rectificación, oposición, limitación del procesamiento, eliminación y derecho a no ser objeto de una decisión individual automatizada, en las condiciones previstas por el RGPD.

Pueden ejercer estos derechos, adjuntando una prueba de su identidad, enviando un correo electrónico a la siguiente dirección: antibribery@edenred.com.

Para cualquier otro tipo de solicitud o reclamación, pueden ponerse en contacto con el Delegado de protección de datos enviando un correo electrónico a data-protection@edenred.com. También le recordamos que pueden presentar una reclamación en relación con el procesamiento de sus datos personales ante la autoridad local de protección de datos personales, como la Comisión Nacional Francesa de Protección de Datos (www.Cnil.fr) en Francia o la Agencia Española de Protección de Datos (aepd.es) en España.

APÉNDICE

A. Apéndice 1: Flujograma detallado para procesar una alerta