

# EXIDE TECHNOLOGIES

## ("Exide" o "la Empresa")

### Política de protección de datos (la Política)

Es necesario que lea la presente política dado que contiene información importante relativa a usted:

- Los principios de la protección de datos que Exide debe cumplir;
- Lo que constituye información personal (o datos) e información personal sensible (o datos);
- Cómo Exide recopila, utiliza y (finalmente) elimina la información personal e información personal sensible de conformidad con la Política;
- Dónde puede encontrarse más información relativa a la protección de datos; por ejemplo, la información personal que Exide recopila o utiliza, cómo se utiliza, almacena y transfiere la información personal, con qué fines, las medidas que se adoptan para mantener la seguridad de la información personal y durante cuánto tiempo de almacena;
- Sus obligaciones como empleado de Exide en relación a la protección de datos; y
- Las consecuencias del incumplimiento de la presente política.

## 1 Introducción

- 1.1 Exide obtiene, almacena y utiliza información personal (también denominada «Datos personal») relativa a terceros para un conjunto de fines legales específicos, como se establece en las *notificaciones de privacidad de protección de datos* de Exide.
- 1.2 Esta política establece cómo cumplimos con las obligaciones relativas a protección de datos. Además, el objetivo de la presente política consiste en garantizar que el personal, incluidos los trabajadores, así como las agencias temporales de trabajadores, comprenden y cumplen las normativas que regulan la recopilación, el uso y la eliminación de la información personal a la que es posible que tengan acceso en el transcurso de las relaciones laborales.
- 1.3 Exide se compromete a cumplir con las obligaciones estipuladas por la protección de datos, así como a tener un comportamiento conciso, claro y transparente en relación a cómo obtenemos y utilizamos la información personal, y cómo (y cuando) eliminamos dicha información una vez que ya no resulta necesaria.
- 1.4 En caso de que tenga alguna duda o comentario en relación al contenido de la presente política o si necesita información adicional, póngase en contacto con el correspondiente local de RGPD o con el departamento de Asesoría Jurídica.

## 2 Ámbito de aplicación

- 2.1 Los empleados deben consultar las notificaciones relativas a la privacidad de protección de datos de Exide y, si procediera, al resto de políticas correspondientes, incluida la relativa a la *seguridad de la información y al mantenimiento de registros*, dado que estos documentos contienen información adicional relativa a la protección de datos personales en estos contextos.
- 2.2 Exide revisará y actualizará la presente política de conformidad con nuestras obligaciones en materia de protección de datos. Esta política no forma parte del contrato de trabajo del empleado. Se podrá modificar, actualizar o complementar dicha política en cualquier momento. Difundiremos cualquier modificación realizada sobre la presente política al personal una vez que esta se adopte.

## 3 Definiciones

**Antecedentes penales** Constituye la información personal en materia de antecedentes penales y delitos

<b>Información</b>	Denuncias, procesos y medidas de seguridad relacionadas;
<b>Fallos de seguridad de los datos</b>	Constituyen los fallos de seguridad que suponen la destrucción accidental o ilegal, pérdida, alteración, divulgación o acceso no autorizado a información personal;
<b>Interesados</b>	Constituyen los titulares de la información personal
<b>Información personal</b>	(También denominados datos personales) constituye la información relativa a datos personales que pueden identificarse (de forma directa o indirecta) de esta información;
<b>Tratamiento de información</b>	Constituye la obtención, registro, organización, almacenamiento, modificación, recuperación, divulgación o destrucción de la información, o, en términos más generales, utilizar la información de cualquier forma;
<b>Pseudonomización</b>	Constituye el proceso mediante el cual la información personal se trata de tal forma que no puede utilizarse para identificar al interesado sin la utilización de información adicional, que se almacena de forma independiente y está sujeta a medidas técnicas y organizativas que garantizan que la información personal no puede atribuirse a un interesado identificable.
<b>Información personal sensible</b>	(También denominada «categorías especiales de datos personales» o «datos personales sensibles») constituye la información personal relativa a la raza, origen étnico, opinión política, religión o creencia filosófica, afiliación o no afiliación sindical, condición genética, información biométrica del interesado (Utilizados para identificar al interesado) e información relativa a la salud, vida sexual u orientación sexual del interesado.

#### **4 Principios de la protección de datos**

- 4.1 Exigirá cumplir con los principios de la protección de datos al proceder al tratamiento de información personal:
- 4.1.1 Trataremos la información personal de forma legal, justa y transparente;
  - 4.1.2 Recopilaremos la información personal únicamente con fines específicos, explícitos y legítimos y no procederemos al tratamiento de forma incompatible con estos fines legítimos;
  - 4.1.3 Únicamente trataremos la información personal adecuada, pertinente y necesaria para los fines pertinentes;
  - 4.1.4 Almacenaremos de forma adecuada y actualizada la información personal, y adoptaremos las medidas correspondientes para garantizar que la información personal inadecuada se elimine o corrija sin demora;
  - 4.1.5 Almacenaremos la información personal de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de dicha información; y
  - 4.1.6 Tomaremos las medidas técnicas y organizativas para garantizar que la información personal se almacena de forma segura y protegida del tratamiento indebido y no autorizado, así como contra la pérdida accidental, destrucción o daño.

#### **5 Bases para el tratamiento de información personal**

- 5.1 En relación a cualquier actividad de tratamiento, Exigirá, antes de que comience el tratamiento la primera vez, y posteriormente mientras este continúe:
- 5.1.1 Revisará los fines de la actividad de tratamiento concreta y seleccionará la base (o bases) lícitas más adecuadas para el tratamiento; por ejemplo:
    - (a) Que el interesado dé su consentimiento para el tratamiento;

- (b) Que el tratamiento sea necesario para la formalización de un contrato del cual el interesado sea parte o para adoptar medidas requeridas por el interesado antes de formalizar un contrato;
  - (c) Que el tratamiento sea necesario para el cumplimiento de las obligaciones legales a las que la empresa está sujeta;
  - (d) Que el tratamiento es necesario para protección de los intereses vitales del interesado o cualquier otra persona natural; o
  - (e) Que el tratamiento sea necesario para los intereses legítimos de Exide o aquellos de la Empresa o un tercero, excepto cuando estos intereses están anulados por los intereses de derechos y libertades fundamentales del interesado—ver cláusula 5.2 a continuación.
- 5.1.2 Salvo que el tratamiento esté basado en el consentimiento, nos cercioramos de que el tratamiento es necesario para el cumplimiento de la base lícita pertinente (por ejemplo, que no existe otra forma razonable de alcanzar este objetivo);
- 5.1.3 Documentar nuestra decisión sobre qué base legal se aplica, para ayudar a demostrar nuestro cumplimiento normativo con los principios de protección de datos;
- 5.1.4 Incluir información tanto sobre los fines del tratamiento como sobre la base legal para ello en nuestra(s) notificación(es) de privacidad pertinente(s);
- 5.1.5 Cuando se trata información personal sensible, identificar también la condición especial lícita para el tratamiento de la información (ver párrafo 6.2.2 a continuación) y documentarla (únicamente para Reino Unido); y
- 5.1.6 Cuando se proceda al tratamiento de información sobre antecedentes penales en virtud del Derecho de la Unión o de los Estados miembros, identificar además una condición legal para el tratamiento de tal información y documentarla.
- 5.2 Al determinar si los intereses legítimos de la Empresa constituyen la base más adecuada para la licitud del tratamiento:
- 5.2.1 Elaboraremos una evaluación adecuada de interés legítimo (LIA) y almacenaremos un registro de la misma para garantizar que podemos justificar nuestra decisión;
  - 5.2.2 En caso de que la LIA identifique una repercusión significativa sobre la privacidad, se considerará si además es necesario elaborar un Estudio de Impacto de Protección de Datos (DPIA), e
  - 5.2.3 Incluir información sobre nuestros intereses legítimos en nuestra(s) notificación(es) de privacidad pertinente(s).

## **6 Información personal sensible**

- 6.1 La información personal sensible en algunas ocasiones se denomina «categorías especiales de datos personales» o «datos personales sensibles».
- 6.2 Es posible que la Empresa necesite proceder al tratamiento de información personal sensible en ciertas ocasiones. Únicamente procederemos al tratamiento de información personal sensible en los casos en los que:
- 6.2.1 Contamos con una base legal para el tratamiento como se establece en el párrafo 5.1.1 anterior; por ejemplo, si es necesario para la formalización de un contrato laboral, para el cumplimiento de las obligaciones legales de Exide o para los intereses legítimos de la Empresa; y
  - 6.2.2 Una de las condiciones especiales para el tratamiento de información personal sensible se aplique; por ejemplo:
    - (a) El interesado ha dado su consentimiento explícito;
    - (b) El tratamiento es necesario para los objetivos de ejercicio de los derechos y obligaciones en materia de derecho laboral de Exide o del interesado;
    - (c) El tratamiento es necesario para proteger los intereses vitales del interesado y el interesado no es físicamente capaz de dar su consentimiento;
    - (d) Tratamiento relativo a datos personales que el interesado haya hecho manifiestamente públicos;
    - (e) Que el tratamiento sea necesario para la formulación, ejercicio o defensa de reclamaciones; o

(f) Que el tratamiento sea necesario por razones de interés público relevante.

- 6.3 Exide no procederá al tratamiento de información personal sensible hasta:
- 6.3.1 Que se haya informado a los interesados de forma adecuada (mediante una notificación de privacidad o de otra manera) de la naturaleza del tratamiento, su finalidad y la base legal para ello.
- 6.4 La Empresa no llevará a cabo una toma de decisiones automatizada (incluida la elaboración de perfiles) basada en la información personal sensible de ningún interesado.
- 6.5 La notificación relativa a la privacidad de protección de datos establece los tipos de información personal sensible que Exide procede a tratar, para lo que se utiliza y la base legal del tratamiento.
- 6.6 En lo relativo a la información personal sensible, la Empresa cumplirá con los procedimientos establecidos en los párrafos 6.7 y 6.8 a continuación para garantizar que cumplen los principios establecidos en el párrafo 4 anterior.
- 6.7 **Durante el proceso de contratación:** El Departamento de Recursos Humanos de Exide garantizará que (excepto en los casos en los que la legislación lo estipule de otra forma):
- 6.7.1 Durante el proceso de preselección, entrevistas, diferentes puntos de la toma de decisiones, no se realizan preguntas relativas a información personal sensible; por ejemplo: la raza u origen étnico, afiliación a sindicatos o salud;
- 6.7.2 cualquier formulario de control de igualdad de oportunidades que se cumplimente se almacenará de forma separada del formulario de solicitud del interesado y no podrá ser visualizado por el personal encargado del proceso de preselección, entrevistas o que tome la decisión relativa a la contratación;
- 6.7.3 Las verificaciones relativas al "Derecho de trabajo" se realizan de forma previa a que se haga una oferta de empleo formal, y no durante las primeras fases de preselección, entrevista o toma de decisiones;
- 6.8 **Durante la relación laboral:** el Departamento de Recursos Humanos se encargará del tratamiento de:
- 6.8.1 Información sanitaria a efectos de administrar el subsidio sanitario, llevar registros de ausencias por enfermedad, controlar la asistencia del personal y facilitar las prestaciones sanitarias correspondientes al puesto de empleo;
- 6.8.2 Información personal sensible a efectos de la supervisión de igualdad de oportunidades. Cuando sea posible, esta información se anonimizará; y
- 6.8.3 La información relativa a la afiliación a sindicatos a efectos de administración del personal y gestión de «selección».

## 7 Información relativa a antecedentes penales

Se procederá al tratamiento de la información relativa a antecedentes penales en virtud del Derecho de la Unión o de los Estados miembros.

## 8 Estudio de Impacto de Protección de Datos (DPIAs)

- 8.1 Cuando existen posibilidades de que el tratamiento suponga un riesgo alto para los derechos de protección de datos del interesado (por ejemplo, cuando Exide tiene previsto utilizar un nuevo sistema tecnológico), antes de comenzar el tratamiento, se realizará un DPIA para evaluar:
- 8.1.1 Si el tratamiento es necesario y proporcionado en relación a su finalidad;
- 8.1.2 El riesgo que supone para los interesados; y
- 8.1.3 Qué medidas pueden aplicarse para hacer frente a estos riesgos y proteger la información personal.
- 8.2 Antes de que se implante un nuevo sistema tecnológico, el responsable debe ponerse en contacto con el Departamento de tecnologías de la información para que se lleve a cabo un DPIA.

8.3 Durante el proceso de un DPIA, la empresa recurrirá al asesoramiento y la opinión de cualquier otra parte interesada pertinente.

## **9 Documentación y registros**

9.1 Exide almacenará un registro escrito de las actividades de tratamiento, entre las que se incluyen:

9.1.1 El nombre e información de la entidad jurídica Exide (y si procediera, de otros responsables);

9.1.2 La finalidad del tratamiento;

9.1.3 Una descripción de las categorías de interesados y categorías de datos personales;

9.1.4 Categorías de los receptores de los datos personales;

9.1.5 Si procede, detalles de la transferencia a terceros países, incluida la documentación de las garantías de los mecanismos de transferencia utilizados;

9.1.6 cuando sea posible, programas de conservación; y

9.1.7 Cuando resulte posible una descripción de las medidas de seguridad técnicas y organizativas.

9.2 Como parte de nuestro registro de actividades de tratamiento, documentamos o vinculamos la documentación a:

9.2.1 Información necesaria para las notificaciones de privacidad;

9.2.2 Información sobre consentimiento;

9.2.3 Contratos responsable-encargado;

9.2.4 La ubicación de información personal;

9.2.5 DPIAs; y

9.2.6 Registro de brechas de seguridad.

9.3 En caso del tratamiento de información personal sensible o de información relativa a antecedentes penales, almacenaremos un registro por escrito de:

9.3.1 La(s) finalidad(es) pertinente(s) para las que el tratamiento se lleva a cabo, incluido (cuando proceda) por qué es necesario para tal finalidad;

9.3.2 La base legal para nuestro tratamiento; y

9.3.3 si almacenamos o eliminamos la información personal de conformidad con nuestra política documental y, si no, los motivos para no cumplir con nuestra política.

9.4 Realizaremos revisiones regulares de la información personal que tratamos y actualizamos nuestra documentación de forma correspondiente.

## **10 Derechos de los interesados**

10.1 Los interesados contarán con los siguientes derechos relativos a su información personal:

10.1.1 A que se les informe sobre cómo, por qué y sobre qué base se procede al tratamiento de la información (ver la notificación de privacidad de protección de datos de Exide);

10.1.2 A obtener la confirmación de que se está procediendo al tratamiento de su información, a obtener acceso a ella y a algunos otros datos mediante una solicitud de acceso;

10.1.3 A la corrección de sus datos en caso de error o de información incompleta;

10.1.4 A la eliminación de los sus datos una vez que ya no resulten necesarios para la finalidad con la que se recopilaron/trataron, o si no existen motivos legítimos que prevalezcan para el tratamiento (también denominado «derecho al olvido»);

10.1.5 A la restricción del tratamiento de la información personal cuando puede rebatirse la precisión de la misma, o si el tratamiento es ilegal; y

10.1.6 A la restricción temporal del tratamiento de información personal cuando esta pueda considerarse imprecisa, o cuando haya oposiciones respecto al tratamiento;

- 10.1.7 Cuando sea imprescindible por cuestiones legales, a establecer pautas para la conservación, eliminación y comunicación de sus datos personales tras su fallecimiento.

## **11 Obligaciones de los interesados**

- 11.1 Los empleados son responsables de colaborar con Exide para el mantenimiento de su información personal actualizada. Es posible que usted tenga acceso a la información personal de otros empleados, proveedores y clientes en el transcurso de la relación laboral o de la contratación. En ese caso, la Empresa espera que usted ayude al cumplimiento de las obligaciones relativas a la protección de datos de los correspondientes interesados. En caso de que tenga acceso a información personal, usted deberá:
- 11.1.1 Acceder únicamente a la información personal para la que esté autorizado y únicamente para fines autorizados;
  - 11.1.2 Permitir a otros miembros del personal de Exide a que accedan a la información personal en caso de que cuenten con la autorización adecuada;
  - 11.1.3 Permitir el acceso a información personal a terceros que no constituyen personal de la Empresa únicamente si cuenta con la autoridad específica del Departamento de Recursos Humanos o de Asesoría jurídica para hacerlo;
  - 11.1.4 Mantener la seguridad de la información personal (por ejemplo, mediante el cumplimiento de las normas de acceso a las instalaciones, acceso a los equipos, protección de contraseñas y almacenamiento y destrucción segura de archivos y otras medidas de seguridad establecidas por la Política global de seguridad de la información de la Empresa);
  - 11.1.5 No eliminar la información personal, o los dispositivos que la contengan (o que puedan utilizarse para acceder a ella), de las instalaciones de la Empresa, a menos que se apliquen las medidas de seguridad adecuadas (como la seudonomización, el cifrado o la protección de la contraseña) en pro de la seguridad de la información y del dispositivo; y
  - 11.1.6 No almacenar información personal en unidades lógicas o en dispositivos personales que se utilicen con fines laborales.
- 11.2 Debe contactar con el Departamento de Recursos Humanos o con el Departamento de Asesoría Jurídica si le preocupa o sospecha que uno de los siguientes acontecimientos ha tenido lugar (o tendrá lugar):
- 11.2.1 Tratamiento de datos personal sin una base legal adecuada o, en caso de información personal sensible;
  - 11.2.2 Cualquier brecha de seguridad en virtud de lo establecido en el párrafo 15.1 a continuación;
  - 11.2.3 Acceso a información personal sin la autorización adecuada;
  - 11.2.4 Información personal almacenada o eliminada de forma insegura;
  - 11.2.5 Eliminación de información personal, o los dispositivos que la contengan (o que puedan utilizarse para acceder a ella), de las instalaciones de la Empresa, sin que se apliquen las medidas de seguridad adecuadas;
  - 11.2.6 Cualquier otro uso indebido de esta política o de cualquiera de los principios establecidos en el párrafo 4.1 enunciado en lo anterior.

## **12 Acceso de interesados**

- 12.1 El interesado podrá solicitar en cualquier momento una solicitud («SAR») para conocer los datos personales que la Empresa conserve sobre él. Normalmente, la Empresa está obligada a responder a las SAR en el plazo de un mes a partir de su recepción (este plazo puede ampliarse hasta dos meses en caso de solicitudes complejas o numerosas. En tal, caso se informará al interesado de la necesidad de dicha ampliación del plazo).
- 12.2 Todas las solicitudes de acceso de titulares recibidas deben ser remitidas al Corresponsal local de GDPR.
- 12.3 La Empresa no cobra ninguna tarifa por la gestión común de las SAR. Exide se reserva el derecho de cobrar honorarios razonables por copias adicionales de información que ya se haya

emitido a un interesado, o en caso de solicitudes manifiestamente injustificadas o excesivas, en particular cuando dichas solicitudes se reiteren

### **13 Seguridad de la información**

- 13.1 La Empresa tomará las medidas técnicas y organizativas para garantizar que la información personal se almacena de forma segura y, en concreto, para prevenir el tratamiento indebido y no autorizado, así como la pérdida accidental, destrucción o daño. Esto puede incluir:
- 13.1.1 Garantizar, si procede, que la información personal se pseudonimice o se encripte;
  - 13.1.2 Garantizar la confidencialidad, la integridad, la disponibilidad y la solidez de carácter permanente de los sistemas y servicios de tratamiento;
  - 13.1.3 Garantizar que, en caso de incidente físico o técnico, la disponibilidad y acceso a la información personal podrá restablecerse de forma puntual; y
  - 13.1.4 Un proceso de comprobación regular, evaluando y valorando la efectividad de las medidas técnicas y organizativas para garantizar la seguridad en el tratamiento.
- 13.2 Cuando la Empresa procede al tratamiento de información personal mediante organizaciones externas en su representación, es necesario llevar a cabo medidas de seguridad adicionales en los contratos con estas organizaciones para salvaguardar la seguridad de la información personal. En concreto, los contratos con organizaciones externas contemplarán que:
- 13.2.1 La organización solo podrá seguir las instrucciones por escrito de Exide;
  - 13.2.2 El tratamiento de los datos está sujeto a una obligación de confidencialidad;
  - 13.2.3 Se tomarán las medidas adecuadas para garantizar la seguridad del tratamiento;
  - 13.2.4 Los subcontratistas únicamente se contratarán con el consentimiento previo de Exide y en virtud de un contrato por escrito;
  - 13.2.5 La organización ayudará a Exide a facilitar el acceso de los interesados y a permitir que estos ejerzan sus derechos en relación con la protección de datos;
  - 13.2.6 La organización prestará asistencia a Exide en el cumplimiento de sus obligaciones en materia de seguridad del tratamiento, notificaciones de fallos en la seguridad de los datos personales y evaluaciones del impacto sobre la protección de los datos;
  - 13.2.7 La organización eliminará o devolverá la información personal a Exide como se establezca en la fecha de vencimiento del contrato; y
  - 13.2.8 La organización se someterá a auditorías e inspecciones, proporcionará a Exide la información que necesite para garantizar que tanto Exide como la organización cumplen con sus obligaciones en materia de protección de datos; y
  - 13.2.9 La organización notificará inmediatamente a Exide si se le solicita que actúe infringiendo la ley de protección de datos.
- 13.3 Antes de que se celebre un nuevo acuerdo que implique el tratamiento de datos personales por parte de una organización externa, o se modifique un acuerdo existente, el personal correspondiente deberá solicitar la aprobación de sus términos al Departamento de Asesoría Jurídica de Exide.

### **14 Almacenamiento y retención de información personal**

- 14.1 La información personal (y la información personal sensible) se almacenará de forma segura de acuerdo con la Política Global de Seguridad de la Información.
- 14.2 La información personal (e información personal sensible) no deberá almacenarse más del periodo necesario. La duración del periodo de almacenamiento de datos dependerá de las circunstancias, incluidos los motivos por los que se ha obtenido la información personal. Los empleados deben seguir la Política de retención de registro de la Empresa, la cual establece el periodo pertinente de retención, o el criterio que debe emplearse para determinar el periodo de retención. En caso de que existan dudas, el personal deberá consultar con el corresponsal local de RGPD o con el departamento de Asesoría Jurídica.

### **15 Brechas de seguridad**

- 15.1 Una brecha de seguridad puede manifestarse de diferentes formas, como, por ejemplo:

- 15.1.1 Pérdida o robo de datos o equipos en los cuales se almacena la información personal;
  - 15.1.2 el acceso no autorizado o el uso de información personal ya sea por parte de un miembro del personal o por parte de un tercero;
  - 15.1.3 Pérdida de datos debido a fallos en los equipos o sistemas (incluido hardware y software);
  - 15.1.4 Fallo humano, como eliminación accidental o alteración de datos;
  - 15.1.5 Circunstancias imprevistas, como incendios e inundaciones;
  - 15.1.6 Ataques deliberados al sistema informático, como la piratería, virus o suplantación de identidad; y
  - 15.1.7 Cuando la información se obtiene mediante la estafa de la organización que la posee.
- 15.2 La Empresa:
- 15.2.1 presentará el informe requerido sobre la brecha de seguridad a la Autoridad de control apropiada o a la Oficina del Comisionario de Información (Reino Unido) sin demoras injustificadas y, cuando sea posible, dentro de las 72 horas siguientes a tener conocimiento de la misma, si es probable que suponga un riesgo para los derechos y libertades de los interesados; y
  - 15.2.2 notificará a los interesados afectados si una brecha de seguridad puede suponer un alto riesgo para sus derechos y libertades y en caso de que la ley exija su notificación.

## **16 Transferencias internacionales**

- 16.1** La Empresa podrá transferir información personal fuera del Espacio Económico Europeo (EEE) (que comprende los países de la Unión Europea e Islandia, Liechtenstein y Noruega) a la última empresa matriz de la Empresa, Exide Technologies en los Estados Unidos de América, partiendo de la base de que Exide Technologies está designada como titular de las cláusulas tipo de protección de datos.

## **17 Formación**

La Empresa se asegurará de que el personal reciba la formación adecuada en relación con sus responsabilidades en materia de protección de datos. Los empleados cuyas funciones requieran un acceso regular a la información personal, o que sean responsables de implantar esta política o de responder a las solicitudes de acceso de los titulares en virtud de la presente política, recibirán formación adicional para como explicación adicional en relación con sus obligaciones y cómo cumplirlas.

## **18 Consecuencias derivadas del incumplimiento**

- 18.1** El cumplimiento de la presente política es de vital relevancia para la empresa. El incumplimiento de la misma:
- 18.1.1 Supone un riesgo para los interesados, cuya información personal es tratada; y
  - 18.1.2 Conlleva el riesgo de sanciones civiles y penales significativas tanto para el empleado como para la empresa; y
  - 18.1.3 Puede, en algunas circunstancias, constituir un delito penal para el empleado.
- 18.2** Dada la importancia de la presente política, el incumplimiento por parte de un empleado de cualquier requisito de la misma puede dar lugar a una acción disciplinaria en virtud de nuestros procedimientos, la cual puede resultar en despido por falta grave. En caso de incumplimiento de la presente política por parte de un tercero que no sea un empleado, podría suponer la resolución de su contrato con efecto inmediato.
- 18.3** Si tiene alguna pregunta sobre cualquier aspecto de esta política, no dude en ponerse en contacto con el Representante nacional RGPD o con el departamento de Asesoría Jurídica.