FARMINGTON INVESTMENT, S.L.
Hotel Puerta América
Avda. de América, 41
28002 Madrid

REGLAMENTO PARA LA IMPLANTACIÓN Y DESARROLLO DEL SISTEMA INTERNO DE INFORMACIÓN DE LA EMPRESA FARMINGTON INVESTMENT, S.L., CON CIF B87531547 DE ACUERDO CON LO ESTABLECIDO 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.

Introducción.-

La Ley 2/2023 incorpora al Derecho español la Directiva (UE) 2019/1937 relativa al régimen del denunciante en el seno se las entidades tanto públicas como privadas. Con ello se pretende proteger a los ciudadanos informantes de las represalias que puedan sufrir, cuando informen sobre vulneraciones del ordenamiento jurídico en el marco de una relación laboral o profesional.

La citada ley establece la obligación de implantar un sistema interno de información que deberá basarse en lo siguiente:

- La implantación de un sistema de efectivo de comunicación basado en un buzón o cauce para recibir la información del denunciante.
- Designar a un Responsable del sistema de información.
- Establecer un procedimiento para recibir y tramitar las denuncias.

La Ley establece que los informantes deben contar con un régimen específico de protección frente a las represalias o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes.

La configuración del Sistema interno de información deberá reunir determinados requisitos, entre otros, uso asequible, garantías de confidencialidad, prácticas correctas de seguimiento, investigación y protección del informante. Asimismo, resulta indispensable para la eficacia del Sistema interno de información, la designación de un responsable con suficientes conocimientos y capacidad para su correcto funcionamiento.

En otro ámbito, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que: «Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable»

La norma europea impone a los Estados miembros la obligación de establecer canales de comunicación adecuados, de modo que su actuación esté presidida por los principios de independencia y autonomía en la recepción y tratamiento de la información sobre las infracciones.

Sobre la base de lo anteriormente relatado, la dirección de FARMINGTON INVESTMENT, S.L., en adelante "**Hotel Puerta América**" o **"Empresa"**, previa consulta a la representación legal de los trabajadores, procede a la redacción y publicación del presente Reglamento del Sistema Interno de Información, de obligado cumplimiento para todo el personal de la empresa y terceros relacionados, cuya entrada en vigor será el 1 de diciembre de 2023.

Artículo 1.- Objeto

El presente documento informativo tiene como objetivo 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 la legislación vigente, a través de los procedimientos previstos en la misma.

También tiene como finalidad el fortalecimiento de la cultura de la información, de la infraestructura de integridad de la Empresa y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas de cualquier tipo.

Artículo 2.- Alcance y aplicación

El contenido del presente documento protege a las personas físicas que informen, a través de alguno de los procedimientos previstos en la Empresa de:

a) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

b) La protección para las personas trabajadoras que informen sobre infracciones del Derecho laboral, derecho penal, en materia de seguridad y salud en el trabajo o cualquier otro hecho ilícito, se entiende sin perjuicio de la establecida en su normativa específica.

c) Esta protección no será de aplicación a las informaciones que afecten a la información clasificada. Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.

Artículo 3.- Ámbito personal de aplicación

1. Se aplicará a los informantes que trabajen en el Hotel Puerta América o terceros 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 por cuenta ajena
    b) Los autónomos
    c) Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la Empresa, incluidos los miembros no ejecutivos
    d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

2. También se aplicará a los informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, trabajadores en periodos de prácticas con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral

todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

3. Las medidas de protección del informante también se aplicarán, en su caso, específicamente a los representantes legales de los trabajadores en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

4. También serán de aplicación, en su caso, a:

   a) Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.

   b) Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.

   c) Personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.

Artículo 4.- Sistema interno de información

1. El órgano de administración de la Empresa, es el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de los trabajadores, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en el RGPD y en la LOPDGDD.

2. El Sistema interno de información, en cualquiera de sus fórmulas de gestión, permitirá:

   a) A todas las personas comunicar información sobre cualquier infracción.

   b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice 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) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

   d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la Empresa.

   e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la Empresa con el objetivo de que el primero en conocer la posible irregularidad sea la propia Empresa.

   f) Contar con un responsable del sistema en los términos previstos en la norma.

   g) Contar con una política que enuncie los principios generales en materia de sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la Empresa.

   h) Contar con un procedimiento de gestión de las denuncias recibidas.

   i) Establecer las garantías para la protección de los informantes en el ámbito de la propia Empresa, respetando, en todo caso, lo dispuesto en la norma.

Artículo 5.- Gestión del sistema interno de información por tercero externo

1. La gestión del Sistema interno de información se podrá llevar a cabo dentro de la propia Empresa o acudiendo a un tercero externo. A estos efectos, se considerará gestión del Sistema la recepción de informaciones.

2. La gestión del sistema por un tercero externo exigirá, en todo caso, que este ofrezca garantías adecuadas de respeto a la independencia, confidencialidad, la protección de datos y el secreto de las comunicaciones. El tratamiento de datos por parte de terceros (Encargados del tratamiento), requiere la previa suscripción del acuerdo regulado en el artículo 28 del 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), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. La gestión del Sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema.

Artículo 6.- Canal interno de información

1. El canal interno de información de la empresa para posibilitar la presentación de información respecto de las infracciones previstas en la normativa vigente, estará integrado dentro del Sistema interno de información.

2. El canal interno permitirá realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se puede realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto.

   A solicitud del informante, también puede presentarse mediante una reunión presencial dentro del plazo máximo de siete días. En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece el RGPD. Además, 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.

   Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones que correspondan. Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente, deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

   a) Mediante una grabación de la conversación en un formato seguro, duradero y accesible.

   b) A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

3. Los canales internos de información permitirán incluso la presentación y posterior tramitación de comunicaciones anónimas.

Artículo 7.- Responsable del sistema interno de información

1. El Hotel Puerta América es competente para la designación de la persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.
2. El Responsable del Sistema desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad, no pudiendo recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

Artículo 8.- Procedimiento de gestión de informaciones

1. La empresa aprobará el procedimiento de gestión de informaciones. El Responsable del Sistema, ya sea interno o externo, responderá de su tramitación diligente.
2. El procedimiento establecerá las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos.

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

   a) Identificación del canal o canales internos de información a los que se asocian.

   b) Acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

   c) Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

   d) Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a este información adicional.

   e) Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

   f) Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.

Artículo 9.- Entidades obligadas del sector privado

Están obligadas a disponer un Sistema interno de información en los términos previstos en la ley 2/2023, de 20 de febrero, las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores.

Las personas jurídicas en el sector privado que tengan entre cincuenta y doscientos cuarenta y nueve trabajadores y que así lo decidan, podrán compartir entre sí el Sistema interno de información 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, respetándose en todo caso las garantías previstas en la ley.

Artículo 10.- Instrucción

1. La instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados en la denuncia.
2. Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta, siempre que la comunicación no afecte a la instrucción. Adicionalmente se le informará del derecho que tiene a presentar alegaciones por escrito y sobre el tratamiento de sus datos personales.
3. En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación. Durante la instrucción se informará, sucintamente, de la relación de hechos al investigado. Esta información podrá efectuarse en el trámite de audiencia si se considera que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.
4. Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una entrevista con la persona o personas afectadas en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes.
5. El plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a tres meses desde la entrada en registro de la información. Cualquiera que sea la decisión, se comunicará al informante, salvo que haya renunciado a ello o que la comunicación sea anónima.

Artículo 11.-Informción sobre los canales interno y externo de información

Los sujetos comprendidos dentro del ámbito de aplicación de la ley 2/2023, de 20 de febrero, proporcionarán la información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión.

En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable.

Artículo 12.-Registro de informaciones

La empresa dispondrá de un canal interno de información y deberá contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la normativa vigente. 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.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con el RGPD y de la LOPDGDD.

Artículo 13.-Régimen jurídico del tratamiento de datos personales

Los tratamientos de datos personales que deriven de la aplicación de la ley se regirán por lo dispuesto en el RGPD, en la LOPDGDD y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Artículo 14.-Información sobre protección de datos personales y ejercicio de derechos

1. Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del RGPD y 11 de la LOPDGDD. A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.
2. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.
3. Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
4. En caso de que la persona a la que se refieran los hechos relatados en la comunicación ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Artículo 15.-Tratamiento de datos personales en el sistema interno de información

1. El acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:
   a) El Responsable del Sistema y a quien lo gestione directamente.
   b) El responsable de recursos humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
   c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
   d) Los Encargados del tratamiento que eventualmente se designen.
2. Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.
3. Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.
4. 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 LOPDGDD.

5. Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información.

Artículo 16.-Preservación de la identidad del informante y de las personas afectadas:

1. Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

2. Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

3. La identidad del informante solo podrá ser comunicada a la Autoridad competente en el marco de una investigación penal, disciplinaria o sancionadora.

Artículo 17.-Condiciones de protección

1. Las personas que comuniquen o revelen infracciones previstas en la norma, tendrán derecho a protección siempre que concurran las circunstancias siguientes:

   a) Que tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de la ley 2/2023.

   b) Que la comunicación o revelación se haya realizado conforme a los requerimientos previstos en el artículo 4 de este documento.

2. Quedan expresamente excluidos de la protección prevista en la ley aquellas personas que comuniquen o revelen:

   a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en el artículo 18.2.a) de la Ley 2/2024 de 20 de febrero. La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes.

   b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

   c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

   d) Informaciones que se refieran a acciones u omisiones no comprendidas en el artículo 4 de este documento.

   e) Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones a que se refiere el artículo 4 anterior de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en la ley, tendrán derecho a la protección que la misma contiene.

Artículo 19.- Prohibición de represalias

1. Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en la ley.
2. Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública.
3. A los efectos de lo previsto en este documento, y a título enunciativo, se consideran represalias las que se adopten en forma de:
    a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
    b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
    c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.
    d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.

Artículo 20.- Medidas para la protección de las personas afectadas

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos legalmente previstos, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

Artículo 21.- Plazo máximo para el establecimiento del Sistema interno de información

El plazo máximo para el establecimiento de Sistemas internos de información y adaptación de los ya existentes, en el caso de las entidades jurídicas del sector privado con doscientos cuarenta y nueve trabajadores o menos, será hasta el 1 de diciembre de 2023.

Artículo 22.- Gestión del Sistema Interno de Información

Mediante el presente reglamento, y de acuerdo con lo establecido en el articulo 1.709 y siguientes del código Civil, se otorga mandato especial, tan amplio como en derecho se requiera y sea necesario, al representante legal de DORDIO ASSOCIATES, S.L., para que, de acuerdo con lo establecido en la normativa vigente, además de las actuaciones que deba desarrollar como consecuencia de lo establecido en el reglamento para la implantación y desarrollo del sistema interno de información de la empresa FARMINGTON INVESTMENT, S.L., lleve a cabo, en las condiciones y formas necesarias, cuantas acciones sean legalmente pertinentes para garantizar la protección del patrimonio de la empresa.

El presente mandato especial, alcanza todos los aspectos que sean necesarios tendentes a ejecutar las acciones para cuya finalidad se expide, incluyendo los correspondientes controles de productos y personas que sean necesarios directa, o indirectamente, con el único límite que la legislación vigente establezca.

Que, de igual manera, este mandato especial autoriza al mandatario a comparecer, si fuera necesario, ante las autoridades policiales y/o judiciales que correspondan como consecuencia de las acciones llevadas a cabo.

Artículo 23.- Protección de datos de carácter personal

De acuerdo con lo señalado en el articulo 5 de este reglamento, y para dar cumplimiento a lo establecido en el artículo 28 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), se deja constancia de lo siguiente:

a) Que FARMINGTON INVESTMENT, S.L., Responsable del tratamiento (En adelante: responsable), ha contratado los servicios del DORDIO ASSOCIATES, S.L., Encargado del tratamiento (En adelante Encargado), para implantar y desarrollar el sistema interno de información de la empresa, de acuerdo con lo establecido en la Ley 2/2023 de 20 de febrero.

b) Que, para el cumplimiento del servicio antes señalado, el Encargado tendrá acceso a los datos personales bajo la responsabilidad del Responsable.

c) Que, en cumplimiento de lo dispuesto en el artículo 28 del GDPR, el Encargado ofrece suficientes garantías para implementar políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad que establece la normativa vigente y proteger los derechos de los interesados, por lo cual ambas partes convienen suscribir el presente contrato con sujeción a las siguientes instrucciones para el tratamiento de datos.

1. Objeto, naturaleza y finalidad del encargo

- La finalidad del encargo es la Gestión del sistema interno de información de acuerdo con lo establecido en la Ley 2/2023 de 20 de febrero.
- El deber de informar del tratamiento al interesado corresponderá exclusivamente al Encargado.
- La ubicación del tratamiento será en los locales del Responsable y/o en los locales del Encargado, con autorización del Responsable para incorporar los datos a sus sistemas.

2. Tipo de datos personales y categoría de interesados

- El tipo de datos personales a los que tendrá acceso el Encargado serán DNI/NIF/NIE/Pasaporte, nombre y apellidos, dirección postal o electrónica, teléfono, firma manual.

- Otros tipos de datos serán las características personales, académicos y profesionales, detalles de empleo, económicos, financieros y de seguro, transacciones de bienes y servicios.
- La categoría de los interesados será la de empleados o externos informantes.
- Las operaciones de tratamiento autorizadas son las estrictamente necesarias para alcanzar la finalidad del encargo.

3. Obligaciones y derechos del Responsable

El Responsable garantiza que los datos facilitados al Encargado se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

El Responsable pondrá a disposición del Encargado cuanta información sea necesaria para ejecutar las prestaciones objeto del encargo.

El Responsable advierte al Encargado de que, si determina por su cuenta los fines y los medios del tratamiento, se considerará responsable del tratamiento y estará sujeto a cumplir las disposiciones de la normativa vigente aplicables como tal.

4. Obligaciones y derechos del Encargado

El Encargado se obliga a respetar todas las obligaciones que pudieran corresponderle conforme a lo dispuesto en la normativa vigente y cualquier otra disposición o regulación que le fuera igualmente aplicable.

El Encargado no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al encargo o que suponga el incumplimiento de este contrato.

El Encargado pondrá a disposición del Responsable la información necesaria para demostrar el cumplimiento del contrato, permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento.

5. Personal autorizado para realizar el tratamiento

El Encargado garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos o que está sujeto a una obligación de confidencialidad de naturaleza legal.

El Encargado tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratarlos siguiendo las instrucciones del Responsable o esté obligada a ello en virtud de la legislación vigente.

El Encargado garantiza que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

6. Medidas de seguridad

El Encargado manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de protección de datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del RGPD.

El Encargado garantiza que se implementarán adecuadamente dichas medidas de seguridad y ayudará al Responsable a cumplir las obligaciones establecidas en los artículos del 32 al 36 del GDPR, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del Encargado.

El Responsable realizará un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de los interesados y, si determinara que existen riesgos, trasladará al Encargado un informe con la evaluación de impacto para que proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

El Encargado, por su parte, deberá analizar los posibles riesgos y otras circunstancias que puedan incidir en la seguridad que le sean atribuibles, debiendo informar, si los hubiere, al Responsable para evaluar su impacto.

De todas formas, el Encargado garantiza que, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, implementará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entrañe el tratamiento, que en su caso incluya, entre otros:

- Seudonimización y cifrado de datos personales.
- Garantía de confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restauración de la disponibilidad y el acceso a datos de forma rápida en caso de incidente físico o técnico.
- Procedimientos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

7. Violación de la seguridad

Las violaciones de seguridad de que tenga conocimiento el Encargado deberán notificarse sin dilación indebida al Responsable para su conocimiento y aplicación de medidas para remediar y mitigar los efectos ocasionados. No será necesaria la notificación cuando sea improbable que comporte un riesgo para los derechos y las libertades de las personas físicas.

La notificación de una violación de seguridad deberá contener, como mínimo, la siguiente información:

- Descripción de la naturaleza de la violación.
- Categorías y el número aproximado de interesados afectados.
- Categorías y el número aproximado de registros de datos afectados.
- Posibles consecuencias.
- Medidas adoptadas o propuestas para remediar o mitigar los efectos.
- Datos de contacto donde pueda obtenerse más información (DPO, responsable de seguridad, etc.).

8. Comunicación de los datos a terceros

El Encargado no podrá comunicar los datos a terceros destinatarios, salvo que hubiera obtenido una autorización previa y por escrito del Responsable; la cual, de existir, se anexará al presente contrato.

La transmisión de datos a autoridades públicas en el ejercicio de sus funciones, no es consideradas comunicaciones de datos, por lo que no se precisará la autorización del Responsable si dichas transmisiones son necesarias para alcanzar la finalidad del encargo.

9. Transferencias internacionales de datos

El Encargado no podrá realizar transferencias de datos a terceros países u organizaciones internacionales no establecidos en el EEE, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

10. Subcontratación del tratamiento de datos

El Encargado no podrá subcontratar a un tercero la realización de ningún tratamiento de datos que le hubiera encomendado el Responsable, salvo que este lo autorice de manera previa y por escrito, y quede constancia anexando la autorización al presente contrato.

11. Derechos de los interesados

El Encargado creará, siempre que sea posible y teniendo cuenta la naturaleza del tratamiento, las condiciones técnicas y organizativas necesarias para asistir al Responsable en su obligación de responder a las solicitudes de los derechos del interesado.

En caso de que el Encargado reciba una solicitud para el ejercicio de estos derechos, debe comunicarlo al Responsable de forma inmediata y, en ningún caso, más allá del día laborable siguiente al de la recepción de la solicitud, adjuntando otras informaciones que puedan ser relevantes para resolverla.

12. Responsabilidad

Conforme al artículo 82 del RGPD, el Responsable responderá de los daños y perjuicios causados en cualquier operación de tratamiento en que participe y no cumpla lo dispuesto en el RGPD, y el Encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del RGPD dirigidas específicamente al Encargado o haya actuado al margen o en contra de las instrucciones legales del Responsable. Del mismo modo, el Encargado estará exento de responsabilidad si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

13. Fin de la prestación de servicio

Una vez finalice la prestación de servicios objeto de este contrato, si el Encargado hubiera almacenado datos personales, o cualquier otro documento y/o soporte que se le hubiera facilitado por cualquier medio, deberá devolverlos, suprimirlos o entregarlos a un nuevo Encargado, a elección del Responsable, incluidas las copias existentes. El Encargado deberá emitir un certificado de devolución o destrucción si así lo exigiera el Responsable.

No procederá la supresión de datos cuando se requiera su conservación por una previsión legal, en cuyo caso el Encargado procederá a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con el Responsable.

El Encargado mantendrá el deber de secreto y confidencialidad de los datos incluso después de finalizar la relación objeto de este contrato.

Disposición final única

La dirección de comunicaciones por cualquier medio a los efectos de dar cumplimiento a la ley 2/2023 de 20 de febrero y el artículo 5 del presente reglamento de gestión del sistema de información es la siguiente:

Representante Legal
DORDIO & ASSOCIATES, S.L.
Hermanos García Noblejas, 39
28037 Madrid
Teléfono: 609 177 551
Email: dordio@dordio.es

La entrada en vigor del presente reglamento de Gestión interna de información es el 1 de diciembre de 2023