

Política sobre el Sistema Interno de Información

GRUPO MARK'ENNOVY

1 de Diciembre de 2023

ÍNDICE

1.	¿QUÉ ES EL SISTEMA INTERNO DE INFORMACIÓN DEL GRUPO?	3
2.	VÍAS PARA LA PRESENTACIÓN DE UNA COMUNICACIÓN	4
3.	PRINCIPIOS ESENCIALES DEL SISTEMA INTERNO DE INFORMACIÓN....	5
3.1	CONFIDENCIALIDAD	5
3.2	DERECHO AL ANONIMATO	6
3.3	PROHIBICIÓN DE REPRESALIAS	6
3.4	DERECHOS DE LA PERSONA INVESTIGADA	6
3.5	TRAMITACIÓN EFECTIVA DE LAS COMUNICACIONES RECIBIDAS	7
4.	PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	8
4.1	RESPONSABLE DEL TRATAMIENTO	8
4.2	CATEGORÍAS DE DATOS PERSONALES Y ORIGEN DE LOS DATOS	8
4.3	TRATAMIENTO DE LOS DATOS PERSONALES (FINALIDADES, BASES LEGALES Y PLAZOS DE RETENCIÓN)	9
5.	LIBRO-REGISTRO.....	12
6.	FORMACIÓN Y DIFUSIÓN	12
7.	NORMATIVAS LOCALES APLICABLES	12
8.	RÉGIMEN DISCIPLINARIO.....	13

1. ¿QUÉ ES EL SISTEMA INTERNO DE INFORMACIÓN DEL GRUPO?¹

Mark'envoy Personalized Care, S.L. y sus sociedades filiales (conjuntamente, el "**Grupo**") tienen un firme compromiso con el cumplimiento normativo y la ética empresarial en el desarrollo de su actividad.

Por este motivo, el Grupo ha establecido un sistema interno de información, articulado en torno a un canal a través del cual los profesionales del Grupo o cualquier tercero puedan informar de la posible existencia de una infracción penal o administrativa o de cualquier otro comportamiento ilícito cometido en el marco de la actividad desarrollada por el Grupo que se haya conocido en un contexto laboral o profesional.

El término "**Profesionales**" engloba a todas las personas que conforman el Grupo, incluyendo sus consejeros o administradores, directivos, empleados o becarios. En cualquier caso, como ya se ha indicado, cualquier otra persona física que, en un contexto laboral o profesional, tenga información sobre la posible comisión de la infracción correspondiente podrá hacer uso del canal de comunicación previsto en esta Política. Todas las personas mencionadas en este párrafo serán referidas en lo sucesivo como "**Informante**" o "**Informantes**", respectivamente.

La presente Política sobre el funcionamiento del sistema interno de información (la "**Política**") establece los principios esenciales del Procedimiento de Gestión de Comunicaciones (los detalles del cual han sido compartidos en otro documento) (el "**Procedimiento**"), que resulta aplicable al Grupo de conformidad con lo dispuesto 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 (la "**Ley de Protección de Informantes**").

Tal y como establece el artículo 4 de la Ley de Protección de Informantes, el sistema interno de información que se regula en la presente Política es el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2 del citado texto legal². No obstante, la Ley de Protección de Informantes establece asimismo un canal externo ante la Autoridad Independiente de Protección del Informante, AAI

¹ Esta es la versión original de la presente Política, redactada en español. Además, existe una traducción en inglés. En caso de conflicto, prevalecerá la versión en español.

² Las infracciones que pueden ser objeto de la información son (i) infracciones de Derecho de la Unión Europea cuando entren en el ámbito establecido por el Anexo I de la Directiva (UE) 2019/1937 del Parlamento y del Consejo de 23 de octubre de 2019, afecten a los intereses financieros de la Unión o incidan en el mercado interior; (ii) infracciones administrativas graves o muy graves de acuerdo con el ordenamiento jurídico español; e (iii) infracciones penales.

("AIPI"), o las autoridades competentes que se creen a nivel autonómico, para formular directamente la comunicación correspondiente, sin perjuicio de la posibilidad de dirigirse igualmente al resto de autoridades en su caso competentes en función de la naturaleza de la infracción de la que se trate³, incluyendo las instituciones, órganos u organismos de la Unión Europea que resulten competentes. Así pues, la implantación del sistema interno de información no debe interpretarse como una indicación por parte del Grupo para que sus Profesionales no se dirijan directamente a tales autoridades para reportar la potencial existencia de infracciones normativas.

En todo caso, el canal de denuncias no debe ser utilizado como vía para presentar quejas generales o compartir opiniones personales que no impliquen una sospecha fundada de incumplimiento de la normativa legal o de una norma o política interna del Grupo, ni tampoco para transmitir información vinculada a meros conflictos interpersonales o que afecten únicamente al Informante y a las personas afectadas por la comunicación en relación con hechos que no pueden considerarse desproporcionados en un ambiente normal de trabajo y que no impliquen una infracción de la legislación aplicable o de las normas y políticas internas del Grupo. Todos los demás asuntos que no constituyan materia de comunicación en los términos previstos en esta Política, deberán ser canalizados a través de las vías de comunicación establecidas al efecto por el Grupo conforme a su normativa interna.

2. VÍAS PARA LA PRESENTACIÓN DE UNA COMUNICACIÓN

El canal interno del Grupo engloba las siguientes vías para la presentación de comunicaciones:

(i). Por escrito:

- a. A través del **canal de denuncias digital** puesto a disposición del Grupo por la entidad Whistleblower Software ApS el cual permite formular comunicaciones por escrito. Puede accederse a este canal a

³ Efectivamente, dependiendo de la información de la que se trate, podrá dirigirse la comunicación a distintas autoridades, como por ejemplo la Comisión Nacional de los Mercados y de la Competencia, la Administración Estatal de la Agencia Tributaria, la Comisión Nacional de Mercado de Valores, la Agencia Española de Protección de Datos, etc. o, en su caso, las autoridades penales competentes (Juzgado de Instrucción o de Paz, las Fuerzas o Cuerpos de Seguridad del Estado, de las Comunidades Autónomas o de las Corporaciones Locales, así como el Ministerio Fiscal o, cuando los hechos potencialmente constitutivos de delito afecten a los intereses financieros de la Unión Europea, la Fiscalía Europea).

través del siguiente enlace <https://whistleblowersoftware.com/secure/euclidvisiongroupemea> .

- b. Mediante **correo postal** dirigido al Responsable del Sistema (según definido en apartado 3.5), enviándolo a la siguiente dirección: Avenida Ada Lovelace 12, 28906 Getafe, Madrid, España.

(ii). Verbalmente:

- a. A través del **canal de denuncias digital** puesto a disposición del Grupo por la entidad Whistleblower Software ApS, el cual permite formular comunicaciones, además de por escrito, verbalmente mediante la grabación de un mensaje de voz. Puede accederse a este canal a través del siguiente enlace <https://whistleblowersoftware.com/secure/euclidvisiongroupemea> .
- b. Mediante **llamada telefónica** al Responsable del Sistema.
- c. A solicitud del Informante, mediante una **reunión presencial** con el Responsable del Sistema en un plazo máximo de siete días desde la solicitud.

3. PRINCIPIOS ESENCIALES DEL SISTEMA INTERNO DE INFORMACIÓN

3.1 CONFIDENCIALIDAD

Cualquier persona que participe directa o indirectamente en la tramitación de las comunicaciones y en las correspondientes investigaciones internas deberá respetar la confidencialidad de las comunicaciones recibidas y de la investigación realizada conforme a lo dispuesto en la normativa aplicable. En caso de que una comunicación se realice por una vía distinta del canal regulado en la presente Política ante cualquier Profesional del Grupo, el receptor de la comunicación también estará sujeto a la citada obligación de confidencialidad y deberá remitir la comunicación inmediatamente al Responsable del Sistema.

La garantía de confidencialidad de la identidad del Informante constituye uno de los principios rectores del funcionamiento del sistema interno de información, de modo que esta información no será revelada a ninguna persona distinta de aquellas que participen en la recepción y tramitación de la comunicación o, en su caso, en la valoración e implementación de las medidas correctoras, legales o disciplinarias que resulten pertinentes. En ningún caso se comunicará a la persona investigada o

afectada por la comunicación la identidad del Informante, ni ningún dato personal que indirectamente permita su identificación.

3.2 DERECHO AL ANONIMATO

El canal regulado en la presente Política admite la posibilidad de formular comunicaciones anónimas, sea cual sea la forma en que se realice la comunicación (verbal o escrita). No obstante, el Grupo anima a los Informantes a que se identifiquen, ya que esto facilita la tramitación de las comunicaciones.

3.3 PROHIBICIÓN DE REPRESALIAS

El Informante no podrá ser sancionado ni sufrirá ninguna consecuencia negativa o represalia⁴ (incluyendo su amenaza o tentativa) por el hecho de haber formulado la comunicación. Esta garantía de ausencia de represalias se extiende a las personas físicas y jurídicas vinculadas con el Informante⁵, a las personas físicas que, en el marco de la organización en la que preste servicios el Informante, asistan al mismo en el proceso y a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al Informante. Además, el mero hecho de colaborar con la investigación nunca podrá ser merecedor de sanción, represalia o de ninguna otra consecuencia negativa.

En todo caso, están terminantemente prohibidas las comunicaciones realizadas a sabiendas de su falsedad o sin tener motivos razonables para pensar que la información referida es veraz en el momento en que se realiza la comunicación.

3.4 DERECHOS DE LA PERSONA INVESTIGADA

El investigado tiene derecho a ser informado de las acciones u omisiones que se le atribuyen y a ser oído por el instructor de la investigación interna cuantas veces lo solicite (de forma razonable). No obstante, la comunicación al investigado tendrá

⁴ De acuerdo con lo dispuesto en el apartado 2 del artículo 36 de la Ley de Protección de Informantes, 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*”.

Asimismo, de acuerdo con el apartado 1 del artículo 36 de la Ley de Protección de Informantes, se prohíben todos los actos constitutivos de represalia, quedando incluidas tanto las amenazas como las tentativas de represalia.

⁵ En concreto: (a) personas físicas que estén relacionadas con el Informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del Informante; y (b) 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. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación y deberá ajustarse al principio de confidencialidad de la identidad del Informante. Durante la tramitación de la misma, la persona investigada tendrá derecho a la presunción de inocencia, derecho al honor y los demás derechos previstos en la normativa aplicable.

3.5 TRAMITACIÓN EFECTIVA DE LAS COMUNICACIONES RECIBIDAS

El Director de Recursos Humanos de Mark'envoy Personalized Care, S.L. es la persona responsable de la gestión del sistema interno de información que se regula en el presente Procedimiento, de conformidad con lo previsto en el artículo 8 de la Ley de Protección de Informantes (en adelante, el "**Responsable del Sistema**" o el "**Responsable**").

El Responsable del Sistema se encargará de velar por la implementación efectiva del sistema interno de información del Grupo y de la tramitación diligente de las comunicaciones, actuando de forma independiente y autónoma y disponiendo de todos los medios personales y materiales necesarios para ello.

A este respecto, todas las comunicaciones presentadas a través del canal regulado en la presente Política serán admitidas a trámite, salvo que concurra alguno de los siguientes supuestos:

- (i). cuando los hechos relatados carezcan de toda verosimilitud;
- (ii). cuando los hechos no se refieran a la posible comisión de una infracción penal o administrativa o de cualquier otro comportamiento ilícito o contrario a la normativa legal aplicable o a las políticas internas del Grupo;
- (iii). cuando la comunicación carezca manifiestamente de fundamento (por ejemplo, cuando estén basados en meras opiniones personales carentes de indicio de veracidad alguno) o existan indicios racionales de que la información que la sustenta se ha obtenido mediante la comisión de un delito; y
- (iv). cuando la comunicación se refiera a hechos objeto de una comunicación previa y no contenga información nueva y significativa que justifique su tramitación.

Sin perjuicio de la decisión sobre la admisión a trámite de la comunicación, dentro de los siete días naturales siguientes a su recepción se remitirá acuse de recibo de la comunicación al Informante, salvo que ello pueda poner en peligro la confidencialidad de la información.

Se permite la posibilidad de mantener la comunicación con el Informante y, si se considera necesario, de solicitarle información adicional sobre los hechos comunicados. Así, el Informante podrá indicar un domicilio, dirección de correo electrónico o lugar seguro a efectos de recibir las comunicaciones correspondientes.

Las comunicaciones admitidas a trámite serán gestionadas de forma efectiva y estudiadas con detenimiento a fin de adoptar las medidas que, en su caso, se estimen pertinentes.

El Responsable del Sistema deberá velar por que no concurra ninguna situación de conflicto de interés, real o potencial, en la tramitación de las comunicaciones en aras de garantizar que se gestionen con máxima imparcialidad y objetividad.

El plazo máximo para dar respuesta al Informante sobre las actuaciones de investigación se establece en tres meses a partir de su recepción, salvo casos de especial complejidad que requirieran una ampliación del plazo, en cuyo caso este podrá extenderse hasta un máximo de otros tres meses adicionales.

4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

4.1 RESPONSABLE DEL TRATAMIENTO

Cada sociedad del Grupo con la que los Informantes o cualquier otro tercero involucrado en el desarrollo de las investigaciones internas tengan una relación laboral, contractual o de cualquier otra índole, tendrán la consideración de responsables del tratamiento de los datos personales derivado del uso del sistema interno de información y la tramitación de investigaciones internas (los "**Datos Personales**") de conformidad con esta Política y con lo previsto en la normativa sobre protección de datos personales.

El Delegado de Protección de Datos es el punto de contacto el Grupo y, en su caso, con cada sociedad del Grupo, en su calidad de entidad responsable del tratamiento, para cuestiones relativas al tratamiento de datos personales. Si lo desea, el interesado puede contactar con él en la siguiente dirección de correo electrónico privacy@auratechlegal.es

4.2 CATEGORÍAS DE DATOS PERSONALES Y ORIGEN DE LOS DATOS

Los Datos Personales que se tratarán en el ámbito del sistema interno de información serán datos identificativos, de contacto, económicos, profesionales y laborales y relativos a los hechos de los que se informa y, en ocasiones

excepcionales, cuando así sea necesario en el contexto y conforme a la naturaleza de la investigación, datos de categorías especiales (tales como datos relativos a infracciones penales o administrativas, datos de salud, datos sobre la orientación o vida sexual u origen étnico o racial), así como cualquier otro dato derivado del uso y funcionamiento del canal regulado en esta Política.

Los Datos Personales tratados en el ámbito del sistema interno de información serán los aportados directamente por los interesados o, en su caso, por los Informantes, así como por los trabajadores y terceros a los que se solicite información en el transcurso de la investigación, si esta se produce, y que estarán en todo caso relacionados con los hechos investigados.

4.3 TRATAMIENTO DE LOS DATOS PERSONALES (FINALIDADES, BASES LEGALES Y PLAZOS DE RETENCIÓN)

4.3.1 Finalidades del tratamiento y base de legitimación del sistema interno de información

Los Datos Personales serán tratados con el fin de procesar la comunicación y decidir sobre su admisión o inadmisión y, en caso de admisión, llevar a cabo la investigación correspondiente y adoptar las medidas correctoras y disciplinarias que puedan corresponder.

Estos tratamientos de datos se realizarán con base en (a) para las entidades del Grupo obligadas a tener un sistema interno de información por la Ley 2/2023 y el resto de normativa que resulte aplicable (la "**Normativa de Protección de Informantes**"), el cumplimiento de las obligaciones legales; y (b) para aquellas entidades del Grupo que no se encuentran obligadas a mantener un sistema interno de información por la Normativa, el cumplimiento de una misión en interés público.

De igual manera, y únicamente cuando sea estrictamente necesario para estas finalidades, se podrán tratar categorías especiales de datos por razones de un interés público esencial de acuerdo con el artículo 9.2.g) del Reglamento General de Protección de Datos.

4.3.2 Conservación de Datos Personales en el sistema interno de información

Los Datos Personales solo serán tratados dentro del canal de recepción de comunicaciones por el tiempo necesario para tomar una decisión sobre su admisión y no serán comunicados a terceros, salvo que sea necesario para el buen funcionamiento del sistema o la toma de una decisión respecto a la admisión a trámite de una comunicación.

En particular, cuando la vía de presentación de las comunicaciones a través del canal de recepción de comunicaciones sea oral, el Informante es consciente de que las comunicaciones orales quedarán documentadas (i) mediante grabación de la conversación en un formato seguro, duradero y accesible; o (ii) a través de la posterior transcripción completa y exacta de la grabación de la conversación, en cuyo caso se ofrecerá al Informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Una vez adoptada la decisión sobre su admisión o inadmisión, los Datos Personales serán eliminados del canal de recepción de comunicaciones y, en todo caso, si no se hubiera tomado una decisión al respecto, transcurridos tres meses desde su registro. No obstante, podrá conservarse información limitada durante más tiempo con el fin de dejar evidencia del funcionamiento del sistema.

4.3.3 Tramitación de la investigación interna y conservación posterior de Datos Personales

En caso de que la comunicación sea admitida a trámite, los Datos Personales podrán tratarse fuera del canal de recepción de comunicaciones con la finalidad de llevar a cabo la investigación interna pertinente. Este tratamiento se realizará (i) para las entidades del Grupo obligadas a tener un sistema interno de información conforme a la Normativa de Protección de Informantes (aquellas que cuenten con más de 49 empleados), con base en el cumplimiento de obligaciones legales de dichas sociedades (art. 6.1.c) RGPD); y (ii) para las entidades del Grupo que no se encuentren obligadas a mantener un sistema interno de información por la Normativa de Protección de Informantes, para cumplir una misión en interés público (art. 6.1.e) RGPD).

Los Datos Personales serán tratados por el tiempo necesario para llevar a cabo la investigación y cumplir con obligaciones legales.

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 correspondiente procedimiento judicial.

Una vez concluida la investigación, los Datos Personales serán conservados por el tiempo necesario para adoptar y ejecutar las medidas que correspondan y, tras ello, por el plazo máximo de prescripción de cualesquiera acciones legales o contractuales. En ningún caso se conservarán los datos por un período superior a diez años.

4.3.4 Destinatarios de los Datos Personales y transferencias internacionales

Los Datos Personales serán tratados por el Responsable del Sistema y aquellas personas del Grupo que, de conformidad con el ámbito de sus competencias y funciones, y de conformidad con la Ley de Protección de Informantes, sea necesario. Solo serán comunicados a terceros cuando fuera apropiado para llevar a cabo la investigación (p. ej., proveedores de servicios o asesores externos) o para la adopción de las medidas correctivas correspondientes (p.ej., el responsable de recursos humanos —cuando proceda adoptar medidas disciplinarias contra un trabajador— o el responsable de los servicios jurídicos —si procediera adoptar medidas legales en relación con los hechos relatados— del Grupo).

La identidad del Informante podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. Las revelaciones hechas a estos efectos estarán sujetas a salvaguardas expuestas en la normativa aplicable. En particular, se trasladará esta circunstancia al Informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

Si los hechos informados o posteriormente investigados tuvieran circunstancias que hicieran necesaria la transferencia internacional de Datos Personales, se adoptarán las medidas adecuadas conforme a la normativa aplicable. Asimismo, en caso de que el tratamiento de datos por alguno de los prestadores de servicios que asistan en la gestión del canal de recepción de comunicaciones regulado en la presente Política o de la investigación implicara transferencias internacionales, estas se realizarán en todo caso de conformidad con la normativa aplicable. Por ejemplo, se adoptarán cláusulas contractuales tipo aprobadas por la Comisión Europea o se transferirán los datos personales a países para los que la Comisión Europea ha reconocido que proporcionan un adecuado nivel de protección de los datos personales. Se podrá solicitar información sobre las garantías adoptadas por el Grupo contactando con el Delegado de Protección de Datos.

4.3.5 Ejercicio de derechos de protección de datos personales

Las personas que se vean involucradas en el proceso de tramitación previa o de investigación podrán dirigirse al Responsable del Sistema o bien al Delegado de Protección de Datos a los efectos de ejercer sus derechos de acceso, rectificación, oposición, supresión, portabilidad, limitación o cualesquiera otros derechos reconocidos por la normativa en relación con los datos que figuren en el correspondiente expediente, en los términos previstos en la legislación aplicable.

No obstante, cuando la persona a la que se le atribuyan los hechos o cualquier tercero ejercite su derecho de acceso, no se le comunicarán los datos identificativos del Informante.

Asimismo, los titulares de los Datos Personales pueden presentar una reclamación o solicitud relacionada con la protección de sus Datos Personales ante la correspondiente Autoridad de Protección de Datos, en España, la Agencia Española de Protección de Datos (www.aepd.es).

5. LIBRO-REGISTRO

El Responsable del Sistema tiene la obligación de velar por que se lleve un libro-registro de las comunicaciones recibidas y de las investigaciones internas a que pertenezcan, garantizando los requisitos de confidencialidad y de las obligaciones en materia de protección de datos previstos en esta Política y en la normativa aplicable.

6. FORMACIÓN Y DIFUSIÓN

El contenido de la presente Política será objeto de las acciones de formación y difusión que determine en cada momento el Responsable del Sistema.

Asimismo, se remitirá a los Profesionales del Grupo una copia de la Política al momento en que se incorporen al Grupo. Además, en la página web del Grupo se incluirá una sección específica relativa a la existencia del sistema interno de información en la que constará publicada esta Política.

7. NORMATIVAS LOCALES APLICABLES

La presente Política ha sido elaborada sobre la base de la normativa española aplicable (en particular, la Ley de Protección de Informantes), así como los principios y obligaciones reconocidos en la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión Europea. No obstante, en caso de que la comunicación remitida por el Informante esté sometida a la normativa de otro país, la Política resultará aplicable sin perjuicio del cumplimiento de legislaciones distintas de la española (en su ámbito de aplicación) en la medida en que estas establezcan protecciones o garantías adicionales a las previstas en ella.

Si alguna de las previsiones incluidas en esta Política fuera contraria a la normativa local aplicable, se cumplirá con lo dispuesto en dicha normativa.

8. RÉGIMEN DISCIPLINARIO

El incumplimiento de lo dispuesto en la presente Política podrá dar lugar a la imposición de sanciones disciplinarias o a las actuaciones que procedan según la relación que el infractor mantenga con el Grupo.

* * *