POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

DORNA GROUP
11 DE MAYO DE 2023

Índice

1. Introducción....2
2. Objeto....2
3. Principios que rigen el sistema interno de información y el canal interno de comunicaciones..3
4. Canales internos integrados en el sistema de información de DORNA....5
4.1. Presentación de comunicaciones....6
4.2. Garantías del canal interno de comunicaciones....6
4.2.1. Garantías del informante....6
4.2.2. Garantías de la persona afectada....7
5. Modificación de la Política del Sistema Interno de Información....8
6. Aprobación y entrada en vigor....8

1. Introducción

La presente **Política es de aplicación** a las sociedades (i) **DORNA SPORTS, S.L.**, con domicilio social en la Calle Príncipe de Vergara, nº 183 de Madrid – C.P. 28002 y CIF B- 84760800, (ii) **DORNA WORLDWIDE, S.L.U.**, con domicilio social en la Calle Príncipe de Vergara, nº 183 de Madrid – C.P. 28002 y CIF B-82846320 y (iii) **INTERNATIONAL EVENTS SERVICES, S.L.U.**, con domicilio social en la Calle Príncipe de Vergara nº 183 de Madrid – C.P. 28002 y CIF B- 82626144 (en adelante, "**DORNA**").

Con la entrada en vigor de las reformas del Código Penal que conforman el marco legal de la responsabilidad penal de las personas jurídicas en nuestro ordenamiento jurídico, introducidas por la Ley Orgánica 5/2010, de 22 de junio, la Ley Orgánica 1/2015, de 30 de marzo y la reciente Ley Orgánica 1/2019, de 20 de febrero las empresas se han visto en la necesidad de implementar sistemas de cumplimiento normativo eficaces a fin de detectar y en definitiva evitar la comisión de delitos en el desarrollo de sus actividades habituales.

En este contexto, se ha producido la transposición de la Directiva 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.

La aprobación de 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, estipula la obligación de las empresas que reúnan las condiciones previstas de contar con un sistema interno de información que permita comunicar las acciones u omisiones establecidas en el referenciado texto legal.

Adicionalmente, con este documento se da cumplimiento a lo dispuesto por la cláusula 9.1.3 "Fuentes de opinión sobre el desempeño de Compliance" y 10.1.2 "Escalado de Información" de la norma ISO 19600:2015 y a lo dispuesto en el apartado 8.7. "Comunicación de incumplimientos e irregularidades" y el 8.8. "Investigación de incumplimientos e irregularidades de la norma UNE 19601:2017".

En el mismo sentido, se configura la presente Política con base en las últimas reformas normativas operadas por Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Objeto

La presente Política del Sistema Interno de Información tiene por objeto enunciar los principios generales en materia del sistema interno de información y las garantías de defensa del informante y la persona afectada por la comunicación.

El contenido de la presente Política es de obligado cumplimiento para todos los miembros, empleados y profesionales de las sociedades que conforman **DORNA** a cuyo objeto se pone a su disposición.

Asimismo, dispondrán de la posibilidad de informar sobre infracciones en un contexto laboral o profesional cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores de DORNA.

Los empleados y miembros de DORNA tendrán la obligación de utilizar los canales internos de información puestos a su disposición para poner en conocimiento de la entidad cualquier incumplimiento tanto de la legalidad como de su normativa interna del que puedan tener conocimiento.

Por ende, puede decirse que la presente Política del Sistema Interno de Información tiene por objeto completar y adaptar los procedimientos de políticas internas sobre comunicaciones de DORNA y, en definitiva, mejorar el sistema de gestión implementado en DORNA, de acuerdo con el compromiso con la mejora continua de la función de compliance demostrado por la compañía.

En este sentido, la Política del Sistema Interno de Información de DORNA se encuentra ampliamente relacionada con el Procedimiento de Gestión de la Información Recibida, que establece los mecanismos para la gestión y resolución de la comunicación efectuada por el informante.

A efectos del presente Procedimiento, tendrán la consideración de aspectos susceptibles de comunicación, entre otros, los siguientes:

- Acoso, conductas hostiles u ofensivas;
- Actuaciones relacionadas con posibles irregularidades en la relación con proveedores y/o compras; Actuaciones vinculadas con la corrupción pública y privada;
- Apropiación Indebida y Desvío de Recursos;
- Blanqueo de Capitales;
- Apropiación Indebida y Desvío de Recursos;
- Irregularidades e inexactitudes Contables;
- Conflicto de Intereses;
- Compromisos indebidos con terceros;
- Falsificación de documentos, contratos, informes o registros; Vulneración de derechos de empleados, incumplimientos del convenio colectivo aplicable;
- Violaciones de la Seguridad de la Información;
- Cualquier comportamiento que supongan conductas e irregularidades impropias y contrarias a los valores y principios que rigen en DORNA;
- Y, en definitiva, cualquier comportamiento que pudiera contravenir la normativa aplicable, el Código de Conducta o las políticas y procedimientos internos de DORNA.

3. Principios que rigen el sistema interno de información y el canal interno de comunicaciones

Este tipo de procedimientos conllevan aparejados una alta responsabilidad por quién presenta la comunicación, así como el riesgo de estigmatización y vejación de personas dentro de la

organización a la que pertenece. Por este motivo, el sistema interno de información, dentro del programa de prevención de delitos de DORNA, se basa en los siguientes principios:

a) Principio de Independencia:

Los procedimientos a los que den origen las diferentes comunicaciones se regirán por la máxima objetividad e independencia, estableciendo los mecanismos correspondientes de cara a evitar la concurrencia de eventuales conflictos de intereses.

b) Principio de Tolerancia y Respeto:

Como manifestación del máximo rechazo por parte de DORNA a todas aquellas conductas que sean contrarias a sus principios y a la legalidad vigente, se impone la obligación de comunicar el conocimiento de aquellos a todos los miembros de la entidad.

c) Principio de Confidencialidad:

Desde DORNA se garantiza la máxima confidencialidad de las comunicaciones que se reciban y de los datos contenidos en ellas.

Existe prohibición expresa de que los datos personales contenidos en la comunicación sean conocidos por cualquier persona de DORNA que (i) no tenga encargada la gestión de la comunicación o (ii) sea responsable de la aplicación de las medidas cuya ejecución corresponda una vez haya finalizado la investigación.

Lo anterior sin perjuicio de aquellos datos que deban ser revelados a las autoridades en el caso de que la entidad de los hechos o la existencia de algún procedimiento -tanto judicial como ante la administración- así lo requieran.

Así pues, se garantiza 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.

d) Principio de Objetividad y Honradez:

Las actuaciones que ordenan el procedimiento de gestión de las comunicaciones recibidas estarán presididas en todo caso por los principios de absoluta objetividad y máxima honradez.

e) Prohibición de Represalias:

Está absolutamente prohibido adoptar medida alguna contra cualquier persona que emplee los canales internos de comunicación y que suponga una represalia o una consecuencia negativa, con motivo de haber formulado una comunicación de forma debida y con sujeción a las condiciones de uso del canal interno de comunicaciones.

Lo anterior sin perjuicio de la adopción de aquellas medidas que procedan cuando de la investigación interna se desprenda inequívocamente que la comunicación es falsa o malintencionada.

En el supuesto de que se determina que las acusaciones descritas en la comunicación son falsas o maliciosas, en la medida en que hayan sido realizadas de manera deliberada con conocimiento de su falsedad o de forma temeraria, serán consideradas como un incumplimiento grave del presente procedimiento.

En base a lo anterior, DORNA estará legitimada para, respetando el Estatuto de Trabajadores y el convenio colectivo aplicable en caso de los trabajadores y los contratos suscritos en caso de los profesionales, realizar alguna de las acciones recogidas en el apartado número 8 del Procedimiento de Gestión de las Comunicaciones Recibidas.

4. Canales internos integrados en el sistema de información de DORNA

El sistema interno de información implantado por DORNA es un elemento esencial dentro del sistema de gestión de prevención de delitos de la organización, y debe contar, por tanto, con la consideración, respeto y apoyo de todos los integrantes de la compañía.

Respecto de la configuración del sistema interno de información, se encuentra en línea con las exigencias legales establecidas por la Ley 2/2023. Asimismo, observa las recomendaciones formuladas por la Fiscalía General del Estado en su Circular 1/2016. De este texto se deduce la mayor eficacia que se obtiene en la gestión de los mismos, cuando las funciones relativas a la gestión del canal interno de comunicaciones resultan desempeñadas mediante contratación externa. Concretamente se alude a que los mismos resultarán más utilizados y efectivos cuando son gestionados por una empresa externa, ya que garantizan mayores niveles de independencia y confidencialidad.

Es por ello que DORNA ha adoptado un canal interno de comunicaciones, gestionado por ECIJA, como gestor externo del mismo, a través de una herramienta informática -WhistleB, también de un tercero externo - de cara a (i) garantizar el requisito de eficacia de los modelos de organización y gestión en materia de Prevención de Riesgos Penales; (ii) reforzar las medidas de vigilancia y control idóneas para la prevención de comisión de actividades delictivas en el seno de la sociedad, todo ello según lo establecido en el vigente artículo 31 bis del CP, introducido por la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal; y (iii) cumplir con las obligaciones establecidas por laLey 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Asimismo, junto con el canal interno de comunicaciones anteriormente mencionado, se establece la posibilidad en el sistema interno de información de, a solicitud del informante, presentar una comunicación mediante una reunión presencial o telemática dentro del plazo máximo de siete (7) días.

Cuando la comunicación mediante reunión presencial o telemática se realice de forma verbal, deberá documentarse mediante una grabación de la conversación en un formato seguro, duradero y accesible, o a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

4.1. Presentación de comunicaciones

Para facilitar a los miembros de la sociedad y a sus grupos de interés la interposición de comunicaciones, en relación con el conocimiento de conductas contrarias al Código Ético y al sistema de gestión, DORNA ha implementado un canal interno de comunicaciones que se gestiona desde una herramienta externa y se configura del siguiente modo:

i. Software Externo: WhistleB (Software externo sueco que cuenta con los niveles más altos en materia de garantías de anonimato y protección del informante). Que se constituye como medida de aseguramiento de las garantías de protección al informante.
ii. Método de Acceso: **https://report.whistleb.com/dorna, al que se puede acceder desde cualquier dispositivo con conexión a internet.**
iii. Gestor Externo (estándar de eficacia según Circular 1/2016 de la Fiscalía General del Estado): ECIJA. Garantías de autonomía y confidencialidad.

Adicionalmente, se establece la posibilidad en el sistema interno de información de, a solicitud del informante, presentar una comunicación mediante una reunión presencial o telemática dentro del plazo máximo de siete (7) días.

Las comunicaciones presentadas mediante una reunión presencial o telemática recibirán el mismo tratamiento y procedimiento una vez haya sido recibida que las presentadas a través del canal interno de comunicaciones.

Por último, es preciso poner de manifiesto que toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de esta ley, ya sea directamente o previa comunicación a través del correspondiente canal interno.

4.2. Garantías del canal interno de comunicaciones

4.2.1. Garantías del informante

El canal de comunicaciones – como canal interno de información existente en el sistema interno de información de DORNA - dispone de las garantías necesarias para mantener la seguridad de las comunicaciones con el gestor de la comunicación y la preceptiva confidencialidad.

Recibida la comunicación por ECIJA, se procederá primeramente a un examen de imparcialidad y correspondiente ausencia de eventuales conflictos de interés para asegurar que la comunicación es investigada por una persona imparcial en el asunto.

Una vez determinada la imparcialidad y ausencia de conflicto de interés respecto del Compliance Officer de DORNA, se informará sobre la comunicación recibida al Compliance Officer de DORNA y se procederá a la clasificación de la comunicación para que, descartada la posibilidad de que se trate de una comunicación claramente falsa y/o malintencionada, se proceda a realizar las actuaciones instructoras pertinentes.

La investigación de los hechos contenidos en las comunicaciones será gestionada internamente, correspondiendo al Compliance Officer de DORNA, con el apoyo de ECIJA y del área que pudiera corresponder según el tipo de comunicación y los hechos informados, el procedimiento de investigación interna (previa verificación por parte de ECIJA de la ausencia de conflicto de interés según lo dispuesto en los párrafos anteriores).

Las personas encargadas de la gestión de la comunicación recibida tomarán conocimiento del contenido de cada una de las comunicaciones y las tratarán con la diligencia debida, guardando, siempre, la identidad del informante en aquellos supuestos en los que aquella haya sido revelada.

El canal interno de comunicaciones se regirá bajo el principio de máxima confidencialidad, adoptando cuantas medidas sean necesarias de cara a garantiza que no tengan lugar represalias para el informante de buena fe.

4.2.2. Garantías de la persona afectada

Las personas que hayan sido afectadas por la presentación de una comunicación a través del canal interno de comunicaciones nunca podrán ser penalizados por una simple comunicación o notificación a cualquiera de los destinatarios mencionados, siendo, en todo caso, necesario que se compruebe previamente la veracidad de la comunicación y se conceda a las personas implicadas la oportunidad de ofrecer una explicación a la situación comunicada.

Las personas afectadas por la comunicación serán informadas ECIJA y/o por el Compliance Officer, según corresponda, tan pronto como sea posible y, a más tardar, en el plazo de un (1) mes desde la recepción de la comunicación.

En especial, la persona afectada por la comunicación será informada de los siguientes extremos:

- Datos del órgano responsable de la gestión del canal interno de comunicaciones;
- Los hechos comunicados;
- El responsable de tramitar la comunicación;
- Los siguientes hitos que se pueden suceder en el curso de la investigación;
- La información relativa al tratamiento de sus datos de carácter personal.

Excepcionalmente, si existe riesgo importante de que la notificación a la persona afectada por la comunicación ponga en peligro la eficacia de la investigación o recopilación de pruebas, no se

procederá a la notificación hasta que cese dicho riesgo. Quedarán documentados y suficientemente razonados los motivos que inducen a concretar la existencia de dicho riesgo, pudiendo prorrogarse el plazo máximo de un (1) mes previsto por un periodo no superior a tres (3) meses.

La persona afectada tendrá derecho a ser oída en cualquier momento.

Del mismo modo, la información relativa a la persona afectada se tratará con estricta confidencialidad.

5. Modificación de la Política del Sistema Interno de Información

La Política del Sistema Interno de Información deberá ser revisada periódicamente, siendo responsabilidad del órgano de administración, su aprobación y modificación.

6. Aprobación y entrada en vigor.

La Política del Sistema Interno de Información entrará en vigor al día siguiente a su aprobación.