Política del Sistema Interno de Información de SCRM

Fecha de actualización:
01/12/2023
Última revision:
02/02/2024
Supervisor:
Responsable del Sistema Interno de Información (“Responsable del SII”)

SCRM INTERNATIONAL HUB

1 INTRODUCCIÓN

En **SOCIAL BIGDATA COMUNICACIÓN, S.L.U.** (en adelante, la "Organización" o "SCRM") estamos firmemente comprometidos con el buen gobierno, la cultura ética y el cumplimiento de la legalidad vigente. Por ello, en el marco del programa de *compliance* de SCRM y a fin de reforzar la detección de cualquier tipo de incumplimientos, la Organización diseñó y ha venido haciendo uso de distintos canales de comunicación de infracciones que, por medio de la presente política (en adelante la "Política"), se integran en un solo sistema y se adaptan, especialmente, a 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 (en adelante, "Ley de Protección de Informantes"). De este modo, el antiguo canal ético (ahora denominado canal de cumplimiento) y el canal de igualdad y *anti-mobbing & harassment*, ya existentes hasta la fecha, pasan a formar parte de un canal único denominado Sistema Interno de Información (en adelante, , el "Sistema") y, como tal, este Sistema integrado se pone a disposición de todas aquellas personas que se recogen en el apartado 2.2 de la presente Política.

El Sistema contribuye al mantenimiento de la estructura de buen gobierno y de la cultura ética.
A su vez, al permitir la detección temprana de eventuales infracciones, el Sistema también contribuye a proteger a la Organización de eventuales responsabilidades administrativas y penales, así como de los perjuicios reputacionales que se le pudieran ocasionar en virtud de un incumplimiento o infracción. Además, también permite realizar cualquier consulta o comunicación en relación con actuaciones que puedan ser contrarias a la legalidad y/o normativa interna.

En concreto, esta Política ha sido elaborada tomando en consideración la legislación y los estándares normativos siguientes:

Normativa europea

- 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.
- 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 (en adelante, "RGPD").

Normativa española

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, "LOPDGDD").
- Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.
- 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 (en adelante, "Ley de Protección de Informantes").

Estándares

- UNE 19601:2017 de sistemas de gestión de *compliance* penal.

Las comunicaciones realizadas a través del Sistema serán tratadas y resueltas de conformidad con el procedimiento descrito en el punto 4 de la presente Política y respetando las garantías descritas en el apartado 3. Estas garantías serán de aplicación de forma ponderada en función de la tipología de la comunicación.

La presente Política y un *executive summary* de esta estarán a disposición y al alcance de todas las personas empleadas de la Organización.

2 FINALIDAD Y ALCANCE DEL SISTEMA

2.1 Finalidad

La presente Política define los criterios y principios que deben regir en el tratamiento de las comunicaciones realizadas a través del Sistema y que deben ser respetados en la gestión de toda la información recibida a través del mismo, tanto en lo que afecta a las personas que efectúan una comunicación, como a las personas denunciadas.

2.2 Alcance subjetivo

2.2.1 ¿Quiénes pueden realizar una comunicación a través del Sistema?

SCRM pone el Sistema a disposición de los colectivos que se recogen a continuación:

- Todas las personas empleadas de la Organización o de cualquiera de las entidades que forman parte del Grupo Schwarz (en adelante el “Grupo”), incluyéndose, bajo esta denominación, los perfiles de personas directivas, managers, etc..
- Las personas proveedoras, colaboradoras, socios comerciales de SCRM o de cualquiera de las entidades que conforman el Grupo con independencia de que su vinculación se rija por medio de un contrato mercantil o se trate de personas autónomas.
- Las personas que formen parte del órgano de administración o de la dirección de SCRM o de cualquiera de las empresas del Grupo.
- Las personas candidatas que participen en procesos de selección, personas voluntarias, las personas becarias o trabajadoras en formación que formen parte de SCRM o de alguna de las empresas del Grupo.
- Cualquier tercera parte que tenga con interés comercial o profesional legítimo, con independencia de su nivel jerárquico y su ubicación geográfica o funcional.
- También quedan incluidas aquellas personas que comuniquen o revelen públicamente información sobre infracciones.

Los colectivos mencionados se referirán, en adelante, como las “Personas Interesadas”.

Las Personas Interesadas que utilicen el Sistema son responsables de la veracidad de toda la información transmitida y de actuar con buena fe. Se adoptarán las medidas disciplinarias o, en su caso, las medidas que correspondan frente a aquellas personas que presenten comunicaciones o efectúen revelaciones infundadas, falsas, de mala fe, maliciosas o abusivas. En este sentido, también se adoptarán medidas que permitan compensar a las personas que hayan sufrido perjuicios resultantes de comunicaciones o revelaciones infundadas, falsas, de mala fe, espurias o abusivas.

2.2.2 ¿Quiénes pueden ser personas denunciadas a través del Sistema?

Asimismo, SCRM dará trámite a aquellas comunicaciones que se reciban a través del Sistema y que se dirijan contra:

- Personas empleadas de la Organización o de cualquiera de las entidades que forman parte del Grupo, incluyéndose, bajo esta denominación, los perfiles de personas directivas, managers, etc..
- Personas proveedoras, colaboradoras, socios comerciales de SCRM o de cualquiera de las entidades que conforman el Grupo con independencia de que su vinculación se rija por medio de un contrato mercantil o se trate de personas autónomas.
- Las personas que formen parte del órgano de administración o de la dirección de SCRM de o cualquiera de las empresas del Grupo.
- Las personas candidatas que participen en procesos de selección, las personas voluntarias, las personas becarias o trabajadoras en formación que formen parte de SCRM o de alguna de las empresas del Grupo.

Los colectivos referidos en este punto se denominarán, en adelante las "Personas Susceptibles de ser Denunciadas".

2.3 Alcance material

Las Personas Interesadas pueden y deben emplear el Sistema para informar sobre acciones u omisiones cometidas o que estén en proceso de cometerse, en nombre o por cuenta de SCRM, por parte de alguna de las Personas Susceptibles de ser Denunciadas y que puedan constituir un incumplimiento de la normativa legal y/o interna de SCRM y/o del Grupo. En cualquier caso, las Personas Interesadas deben emplear el Sistema, con carácter preferente, para informar de:

- Acciones u omisiones que puedan constituir infracciones de la normativa legal vigente, y especialmente en materia de:
    - Protección de la privacidad y de los datos personales y seguridad de las redes y los sistemas de información.
    - Servicios, productos y mercados financieros, prevención de blanqueo de capitales y financiación del terrorismo.
    - Protección de los consumidores.
    - Salud pública.
    - Seguridad en el transporte.
    - Contratación pública.
    - Protección del medio ambiente, las radiaciones y la seguridad nuclear.
    - Derecho laboral y de seguridad y salud en el trabajo.

- Acciones u omisiones que afecten los intereses de la Unión Europea al incidir en el mercado interior por cuestiones de competencia, actos o prácticas que infrinjan las normas sobre el impuesto de sociedades con el objeto de obtener una ventaja fiscal y ayudas otorgadas por los Estados.
- Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, en particular si comportan un quebranto económico para la Hacienda Pública y para la Seguridad Social.
- Infracciones específicas en materia de igualdad.
- Acciones u omisiones que puedan ser constitutivas de acoso o *mobbing*.

Las cuestiones referidas a la vida personal de las Personas Susceptibles de ser Denunciadas quedan fuera del ámbito del Sistema.

3 GARANTÍAS Y MEDIDAS DE PROTECCIÓN

Las Personas Interesadas que comuniquen irregularidades se beneficiarán de las garantías y medidas que sean de aplicación en función al caso concreto. Todo ello, siempre que la información comunicada sea efectuada de buena fe y sea veraz, clara y fundamentada y, en la medida de lo posible, se reporte acompañada de evidencias que respalden los hechos comunicados.

Si la Persona Interesada ha sido partícipe en la comisión de una infracción administrativa, esta podrá quedar exenta o beneficiarse de una atenuante con respecto a la imposición y cumplimiento de la sanción administrativa que deba ser impuesta por la autoridad competente, siempre y cuando resulte acreditado lo establecido en el artículo 40 de la Ley de Protección de Informantes.

Asimismo, si la Persona Interesada ha sido partícipe en la comisión de una infracción penal, esta podrá beneficiarse de las eximentes o atenuantes de la responsabilidad criminal previstas en los artículos 20 y 21 del Código Penal, siempre y cuando se cumpla lo establecido en dichos artículos.

3.1 Confidencialidad

Se garantiza la confidencialidad de la identidad de cualquier Persona Interesada que haga uso del Sistema, de las personas involucradas en los hechos de los que se haya informado y de las Personas Susceptibles de ser Denunciadas. Asimismo, se velará por la confidencialidad de los hechos y de los detalles del procedimiento, evitando que trasciendan más allá de las personas intervinientes en el mismo.

El Responsable del Sistema será el encargado de velar por la confidencialidad y por el correcto tratamiento y la adecuada gestión de la información facilitada a través del Sistema.

Igualmente, todas las personas que, por ser estrictamente necesario para la gestión apropiada de la comunicación, tengan conocimiento de esta están obligadas a mantener rigurosa confidencialidad con respecto a toda la información, incluyendo los datos de las partes intervinientes en el proceso.

En caso de que la correcta gestión de la investigación interna requiera la participación de medios externos a la Organización (como por ejemplo asesores, consultores u otros profesionales), el Responsable del Sistema también velará por que aquellos se comprometan a guardar la correspondiente confidencialidad de la información y de los datos personales a los que tengan acceso.

No obstante lo previo, para el supuesto de que el resultado de la eventual investigación interna, llevado a cabo a raíz de la información comunicada, se concluya que existen indicios suficientes de la comisión de una conducta constitutiva de delito, una infracción administrativa grave o muy grave o una infracción del derecho de la Unión Europea, se procederá a informar de este extremo tanto a la Persona Interesada, como a la Persona Susceptible de ser Denunciada (salvo que ello pueda comprometer la investigación o el procedimiento judicial) y se trasladará la información del expediente al Ministerio Fiscal, a la Autoridad Judicial o al órgano administrativo competente.

3.2 Comunicación anónima

El Sistema permitirá, en cualquier caso, que la Persona Interesada que quiera hacer uso de este medio pueda realizar la comunicación de forma anónima en caso de que no quiera proporcionar sus datos personales.

Sin embargo, con el fin de facilitar la recolección de información y el avance de la investigación de lo comunicado o alertado mediante el Sistema, resulta conveniente que, aunque la comunicación se produzca de forma anónima, la Persona Interesada indique algún medio seguro a través del que sea posible intercambiar comunicaciones y recabar más información sobre los hechos comunicados en caso de que sea necesario.

3.3 Prohibición de represalias

SCRM garantiza la ausencia de represalias de cualquier índole contra las Personas Interesadas a raíz de cualquier comunicación realizada.

De este modo, se prohíbe que, como consecuencia de las comunicaciones, se impongan amonestaciones, sanciones o despidos improcedentes, entre otros tipos de represalias, o se produzcan tratos desfavorables que puedan perjudicar a las Personas Interesadas, siempre que estas actúen de buena fe.

Cualquier persona empleada o directiva de SCRM que adopte actitudes de represalia contra cualquier Persona Interesada, por haber realizado esta una comunicación de buena fe relativa a una infracción podrá ser sancionada de forma disciplinaria por la Organización. En este sentido, se prohíben y se declaran nulas aquellas conductas que puedan calificarse de represalias y que sean adoptadas dentro de los dos años siguientes a contar desde la finalización de la investigación que haya sido iniciada a consecuencia de una comunicación sobre una infracción. Lo anterior será de aplicación siempre y cuando las Personas Interesadas hayan actuado de buena fe.

Todo ello sin perjuicio de las sanciones administrativas, penales, disciplinarias o de diversa índole que puedan ser impuestas cuando la propia Persona Interesada hubiera participado en los hechos comunicados que constituyeran un incumplimiento o irregularidad que contravenga la normativa interna de la Organización o del Grupo o la normativa legal vigente.

3.4 Derecho a realizar la comunicación de forma escrita, verbal o de ambas formas

Las comunicaciones se pueden realizar a través del Sistema de forma escrita, verbal o de ambas formas. La Persona Interesada también podrá solicitar presentar su comunicación por medio de una reunión presencial, que se celebrará dentro del plazo máximo de 7 días. Si la Persona Interesada opta por la vía de la reunión presencial deberá tener en cuenta que la fecha en que se produzca dicha reunión será la que se tome como referencia para el cómputo de los plazos que afectan a la resolución de la comunicación.

Las comunicaciones realizadas verbalmente, se grabarán o transcribirán, previo consentimiento de la Persona Interesada (a excepción de que ya se hayan remitido en formato de nota de voz).
En cualquier caso, la Persona Interesada tendrá la oportunidad de comprobar, ratificar y aceptar, mediante su firma, la transcripción de la conversación.

3.5 Derecho a obtener respuesta y a completar la comunicación

Las Personas Interesadas que hagan uso del Sistema recibirán un acuse de recibo de la comunicación en el plazo máximo de los 7 días naturales siguientes a la recepción de la comunicación (siempre y cuando las Personas Interesadas hayan facilitado algún dato de contacto que permita el acuse de recibo y salvo que este pueda poner en peligro la confidencialidad de la comunicación).

Asimismo, en caso de que la Persona Interesada haya indicado algún medio seguro, a través del que el Responsable del Sistema pueda intercambiar comunicaciones, el Responsable del Sistema podrá contactar con la persona Interesada con la finalidad de aclarar algún extremo o solicitarle información adicional.

3.6 Derecho a usar otros canales de comunicación

En cualquier momento, la Persona Interesada podrá poner los hechos previamente comunicados a través del Sistema en conocimiento de la Autoridad Independiente de Protección del Informante (la "A.A.I.", en adelante) y/o de los organismos que sean competentes en las Comunidades Autónomas. Asimismo, la Persona Interesada también podrá optar por recurrir directamente a la A.A.I. si lo estima oportuno.

En Cataluña la A.A.I. es la Oficina de Antifraude de Cataluña. Asimismo, en caso de que revista carácter delictivo, la información comunicada también podrá ser puesta a disposición de la Policía, del Ministerio Fiscal o de la autoridad judicial competente.

3.7 Derecho a la información

Las Personas Interesadas que hubieran hecho uso del Sistema enviando cualquier tipo de comunicación o consulta, tendrán derecho a ser informados por parte del Responsable del Sistema de los correspondientes avances y del resultado de la investigación interna, en el concreto caso de haberse iniciado efectivamente dicha investigación.

En caso de no tratarse de la persona directamente perjudicada por los hechos informados, el derecho de información también asiste a las demás personas que hayan sido debidamente identificadas, pudiendo estas solicitar información sobre los avances de la investigación y de las medidas adoptadas. No obstante, el Responsable del Sistema deberá valorar, en cada caso concreto, si resulta procedente informar de tales extremos o no, así como en qué medida se debe informar.

3.8 Derecho al desistimiento en la comunicación

Todas las Personas Interesadas que realicen comunicación mediante el uso del Sistema tendrán derecho a desistir de la misma en caso de no querer seguir con el trámite ordinario de la comunicación.
Por consiguiente, es posible retirar la comunicación una vez realizada.

Sin embargo, si de los hechos comunicados se desprenden indicios razonables de la comisión de algún incumplimiento/irregularidad, el Responsable del Sistema podrá iniciar de oficio un expediente.

4 VÍAS PARA LA REALIZACIÓN DE COMUNICACIONES A TRAVÉS DEL SISTEMA Y PROCEDIMIENTO

Como se adelanta al inicio de la presente política, SCRM dispone de un Sistema, encabezado por un Responsable, que integra los distintos canales internos de información de los que ya disponía la Organización. Es decir, el ahora denominado canal de cumplimiento y el canal de igualdad, *anti-mobbing & harassment*.

El Responsable del Sistema delega la gestión de los referidos canales a la persona que desarrolla las funciones de *compliance Officer* y a la persona Recursos Humanos del modo en que se detalla a continuación.

Asimismo, para garantizar una atención óptima y profesionalizada de todas las comunicaciones que se reciban a través del Sistema, aquellas deberán ser canalizadas siguiendo el siguientela siguiente tabla:

RESPONSABLE DEL SII

SII

CANAL DE CUMPLIMIENTO	CANAL DE IGUALDAD, ANTI-MOBBING & HARASSMENT
GESTIÓN DELEGADA AL COMPLIANCE OFFICER	GESTIÓN DELEGADA AL RESPONSABLE DE HR

¿QUÉ COMUNICAR?

CANAL DE CUMPLIMIENTO

- Incumplimientos de la normativa interna de SCRM o del Grupo.
- Infracciones del Derecho e infracciones administrativas y penales.

CANAL DE IGUALDAD, ANTI-MOBBING & HARASSMENT

- Infracciones en materia de igualdad.
- Acciones u omisiones constitutivas de *mobbing* o acoso.

¿CÓMO COMUNICARLO?

COMUNICACIÓN ESCRITA

CANAL DE CUMPLIMIENTO

E-mail:
Interno: compliance@scrm.lidl
Externo: compliance@filslegal.com

Correo postal:
A/A Compliance
SCRM LIDL International Hub,
Plaza Catalunya,
Calle Bergara 13, Planta 4a,
08002 Barcelona

Online:
Plataforma BKMS
https://www.bkms-system.net/sdl

CANAL DE IGUALDAD, ANTI-MOBBING & HARASSMENT

E-mail:
igualdad@scrm.lidl

Correo postal:
A/A HR
SCRM LIDL International Hub,
Plaza Catalunya,
Calle Bergara 13, Planta 4a,
08002 Barcelona

COMUNICACIÓN VERBAL

CANAL DE CUMPLIMIENTO

Nota de voz a compliance@scrm.lidl
o compliance@filslegal.com

A elección de la Persona Interesada: Entrevista con una de las personas pertenecientes al equipo de Compliance - SCRM.

CANAL DE IGUALDAD, ANTI-MOBBING & HARASSMENT

Nota de voz a igualdad@scrm.lidl

A elección de la Persona Interesada: Entrevista con una de las personas pertenecientes al equipo de HR - SCRM.

4.1 Medios para realizar la comunicación

Tal como se muestra en la tabla anterior SCRM ofrece distintos medios/vías a través de los que las Personas Interesadas pueden hacer uso del Sistema en función de la materia sobre la que se quiera informar y de si la comunicación se realiza de forma escrita o verbalo en función de la mera elección y preferencia de las Personas Interesadas. Estos medios se desarrollan a continuación:

A) Comunicación escrita por correo electrónico interno o externo:

- La comunicación puede canalizarse internamente a compliance@scrm.lidl o, externamente, al abogado de confianza, a través de compliance@filslegal.com cuando las Personas Interesadas informen sobre:
    - Posibles incumplimientos de la normativa interna de SCRM o del Grupo.
    - Posibles infracciones del Derecho / los intereses de la Unión Europea descritas en el apartado 2.3.
    - Posibles infracciones penales o administrativas graves o muy graves.

La persona designada como abogado de confianza es D. Alejandro de Müller, letrado de FILS Abogados S.L.P., con domicilio en Calle Fontcoberta 1-9, 08034 Barcelona.

- La comunicación puede dirigirse internamente a igualdad@scrm.lidl cuando las Personas Interesadas informen sobre:
    - Infracciones específicas en materia de igualdad.
    - Acciones u omisiones que puedan ser constitutivas de acoso o *mobbing*.

B) Comunicación escrita por correo postal:

La comunicación puede remitirse a la siguiente dirección: SCRM – LIDL International Hub, Plaza Catalunya, Calle Bergara no 13, Planta 4a, 08002 Barcelona.

Es importante que la Persona Interesada indique en la parte exterior del sobre si la comunicación debe ser recepcionada por el departamento de *compliance* ("A/A *Compliance*") o por el departamento de Recursos Humanos, en adelante "HR" ("A/A HR"), en función del tipo de información que sea trasladada y según la diferenciación realizada en el diagrama del punto 4 y en el apartado anterior.

C) Comunicación online a través de la plataforma BKMS:

BKMS es la abreviación de Business Keeper Monitoring System. Es un Canal de Denuncias Online que representa una vía segura para las denuncias. Es posible hacerlo de modo anonimo.
Esta vía está dirigida a aquellos supuestos en que la Persona Interesada quiera efectuar una comunicación que se refiera a:

- Posibles incumplimientos de la normativa interna de SCRM o del Grupo.
- Posibles infracciones del Derecho / los intereses de la Unión Europea descritas en el apartado 2.3.
- Posibles infracciones penales o administrativas graves o muy graves.
- Delitos financieros y contra el patrimonio
- Delitos de competencia
- Incumplimiento de la normativa de Protección de Datos
- Violaciones de los derechos humanos y de las normas sociales y medioambientales
- Sospecha de blanqueo de capitales
- Otras infracciones graves de la normativa
- También puede utilizar el canal de denuncias online para aclarar cuestiones concretas de cumplimiento con los miembros del Departamento de Compliance.

https://www.bkms-system.net/sdl

D) Comunicación verbal por nota de voz:

Por parte de SCRM también se ofrece la posibilidad de efectuar una comunicación verbal por medio de la remisión de una nota de voz que deberá enviada a compliance@scrm.lidl o al abogado de confianza, a través de compliance@filslegal.com o a igualdad@scrm.lidl en función del tipo de información que sea trasladada, de acuerdo con la diferenciación efectuada en el diagrama del punto 4 y en el apartado A.

E) Comunicación verbal mediante entrevista reservada:

Para el caso de que la Persona Interesada así lo prefiera, SCRM también ofrece la opción de concertar una entrevista reservada, a agendar en un plazo de 7 días, con el departamento de *compliance* o con el departamento de HR, en función del tipo de información que se quiera trasladar por medio del Sistema.

- La Persona Interesada será atendida por alguien del equipo Compliance - SCRM en aquellos supuestos en que la comunicación a realizar verse sobre:
    - Posibles incumplimientos de la normativa interna de SCRM o del Grupo.
    - Posibles infracciones del Derecho / los intereses de la Unión Europea descritas en el apartado 2.3.
    - Posibles infracciones penales o administrativas graves o muy graves.

- La Persona Interesada será atendida por alguien del equipo HR - SCRM cuando la comunicación a realizar verse sobre:
    - Infracciones específicas en materia de igualdad.
    - Acciones u omisiones que puedan ser constitutivas de acoso o *mobbing*.

4.2 Elementos de la comunicación

A fin de posibilitar el rigor y el avance de la investigación y la confidencialidad en el tratamiento de las comunicaciones estas deberán contener, como mínimo, las siguientes menciones:

- Preferiblemente los datos identificativos de la Persona Interesada que realiza la comunicación, tales como nombre y apellidos, datos de contacto y, en su caso, puesto o número de empleado. No obstante, sin perjuicio de lo anterior, en cumplimiento de lo dispuesto en la Ley de Protección de Informantes, también serán gestionadas aquellas comunicaciones que omitan la identificación de la Persona Interesada por haber sido realizadas anónimamente;
- vinculación de la Persona Interesada con SCRM (por ejemplo: empleado, socio comercial, proveedor, voluntario...etc.);
- datos identificativos de la persona o personas a la que se le imputa el presunto incumplimiento normativo;
- hecho o hechos en que consiste el incumplimiento, concretando la vulneración;
- documentación soporte del incumplimiento, siempre que sea posible; e
- Indicación de la fecha/periodo en el que sucedió en incumplimiento, si el suceso todavía está en curso o si se trata de un evento futuro.

La información aportada deberá ser verosímil y remitida de buena fe por parte de las Personas Interesadas. Del análisis preliminar de dicha información deberán extraerse indicios razonables de la existencia de las infracciones que se comuniquen, así como descartar la posibilidad que se trata de una comunicación de mala fe. Asimismo, será posible mantener la comunicación con la Personas Interesadas y pedir la información adicional cuando se considere necesario.

4.3 Detalle de las personas intervinientes en la recepción y admisión de las comunicaciones

4.3.1 El Responsable del Sistema

Como persona que ha sido designada por el órgano de administración y a quien le han sido concedidos poderes autónomos de iniciativa y control el Responsable del Sistema será el máximo garante de:

- integrar los canales de comunicación de infracciones previamente existente;
- diseñar y establecer el Sistema de modo que sea un canal seguro y libre de injerencias;
- asegurar que el órgano de administración aprueba y mantiene una política/estrategia que enuncia los principios que rigen en materia del Sistema;
- velar por que se apliquen correctamente las garantías recogidas en la presente Política;
- garantizar el funcionamiento óptimo y profesionalizado del Sistema; y
- velar por que el Sistema sea el canal de uso preferente para la canalización de comunicaciones.

SCRM ha dotado al Responsable del Sistema de los recursos personales y materiales necesarios para cumplir sus funciones. Para salvaguardar el funcionamiento óptimo y profesionalizado del Sistema el responsable del mismo procede a:

- delegar y externalizar la gestión del Sistema en el *compliance officer* y su equipo o, en su caso, en el abogado de confianza, en lo relativo al canal de cumplimiento para asegurar la tramitación y resolución profesionalizada de las comunicaciones recibidas por medio del Sistema; y
- delegar la gestión del Sistema en lo relativo al canal de igualdad, anti-*mobbing* y anti-acoso en el Responsable de HR y su equipo a fin de garantizar la tramitación y resolución profesionalizada de las comunicaciones canalizadas a través del Sistema.

Pese a la delegación referida, el Responsable del Sistema sigue siendo el máximo garante de:

- asegurar la gestión diligente del Sistema;
- cerciorarse del cumplimiento de los plazos establecidos en la presente Política y de que se realicen las investigaciones que resulten necesarias;
- velar por que se adopten las medidas necesarias que sean precisas en cada caso; y
- asegurar que el personal que puede recibir una denuncia fuera del canal recibe la recepción de información y formación adecuada.

Además, el Responsable del SII también ostenta una serie de funciones y responsabilidades en su condición de interlocutor frente a las Autoridades. Como tal, deberá:

- atender a los requerimientos que se reciban por parte de la Oficina Antifraude de Catalunya o la A.A.I. correspondiente;
- atender a los requerimientos que se reciban por parte de la Policía Judicial, el Ministerio Fiscal, la Autoridad Judicial o el órgano administrativo competente; y
- remitir al Ministerio Fiscal, a la Autoridad Judicial o al órgano administrativo competente aquellos expedientes en los que se hayan observado indicios suficientes de la comisión de una conducta constitutiva de delito, una infracción administrativa grave o muy grave o una infracción del derecho de la Unión Europea.

4.3.2 El Abogado de confianza

Como órgano externo de admisión y tramitación de las comunicaciones remitidas por la Persona Interesada, el Abogado de confianza realizará las siguientes tareas:

- acusar recibo de la comunicación en el plazo máximo de 7 días naturales desde que se tenga conocimiento de su recepción (siempre que se dispongan los datos del contacto de la Persona Interesada y salvo que ello pueda poner en peligro la confidencialidad de la comunicación);
- verificar, en primer lugar, si las comunicaciones recibidas se encuentran en el ámbito de competencia de SCRM;
- obtener y documentar el consentimiento de la Persona Interesada para el reenvío de la información al Responsable del Sistema o al Delegado de *compliance* del Grupo cuando el aviso afecta a un miembro del órgano de administración o el CEO;
- informar a las Personas Interesadas de la decisión adoptada sobre la admisión o archivo de la comunicación, en el plazo máximo de 3 meses, desde el acuse de recibo, o, si no se hubiese producido dicho acuse de recibo, desde el vencimiento del plazo de 7 días desde la recepción de la comunicación. Todo ello salvo en los casos de especial complejidad que requieran más tiempo para la investigación y donde el plazo de 3 meses podrá extenderse hasta un máximo de otros 3 meses adicionales; y
- cuando los hechos pudieran ser indiciariamente constitutivos de delito lo comunicará de inmediato a SCRM para poder cumplir con la obligación de informar a la autoridad competente. En caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

El Abogado de confianza, tiene el deber de secreto profesional, por lo tanto, comunicará los hechos comprobados y los datos personales de las Personas Interesadas al Responsable del Sistema y, en su caso, al Delegado de *compliance* del Grupo solo con el expreso consentimiento de aquel. Las Personas Interesadas decidirán si, y en qué medida, se revelarán los hechos comunicados y/o su identidad. El consentimiento de las Personas Interesadas se documentará en el formulario de comunicación (Anexo 1).

No obstante, si los hechos comunicados dan motivos para suponer que SCRM puede haber sufrido daños significativos o corre peligro de sufrirlos, el Abogado de confianza deberá comunicarle los hechos, incluso contra la voluntad de la Persona Interesada, manteniendo en lo posible el anonimato de esta. Por daños significativos se entienden especialmente:

- daños personales con riesgo para la vida e integridad física; o
- daños económicos considerables, una vez verificada la envergadura del daño junto con SCRM, después de haber recibido la comunicación en cuestión.

Si la Persona Interesada ha dado su consentimiento para el reenvío de los hechos comunicados, pero no de su identidad, el Abogado de confianza deberá reenviar la comunicación anonimizada. En este caso el Abogado de confianza informará a la Persona Interesada sobre la decisión adoptada por parte de SCRM en el plazo máximo de 3 meses desde el acuse de recibo.

Si la Persona Interesada no ha dado su consentimiento de reenviar los hechos comunicados y no es posible revelarlos sin su consentimiento, salvo en el supuesto de los posibles daños significativos para SCRM, el Abogado de confianza archivará la comunicación.

4.3.3 *Compliance officer* y Responsable de HR

Las comunicaciones realizadas internamente serán recibidas directamente por las personas designadas del equipo de *compliance officer* o, en su caso, del equipo de HR. Esos serán quienes, dependiendo de la materia sobre la que verse la comunicación, acusarán el recibo de las mismas en el plazo máximo de 7 días naturales desde que se tenga conocimiento de su recepción.

Atendiendo a que el Sistema es un canal que integra los canales de comunicación de infracciones que han venido existiendo históricamente en SCRM, se prevé el intercambio de información entre el *compliance officer* y el Responsable de HR, en los dos supuestos siguientes:

- cuando la Persona Interesada haya remitido una comunicación por la vía equivocada y, por razón de la materia, deba ser tratada por los profesionales del otro equipo: En este caso, el responsable del equipo receptor, pero no competente trasladará el expediente al responsable del otro equipo y lo hará a la mayor brevedad y, en cualquier caso, antes de que transcurra el plazo legal de 7 días naturales establecidos para el acuse de recibo; o
- cuando la infracción comunicada por medio de uno de los canales contenga (aunque sea de forma parcial) elementos del ámbito de competencia y responsabilidad del otro equipo: En este caso se involucrará en la investigación al equipo en cuestión.

Este intercambio de información no afectará en ningún caso a la confidencialidad con la que debe tratarse el expediente en cuanto a su contenido y sus intervinientes.

A) A continuación, el *compliance officer*/ Responsable de HR comprobará:

- si la comunicación recae dentro del ámbito de competencia de SCRM y del alcance del Sistema, en cuyo caso abrirá el correspondiente expediente. Para garantizar una atención óptima y profesionalizada de todas las comunicaciones recibidas a través del Sistema, y como ha sido indicado en los apartados 4 y 4.1, el Responsable del Sistema será asistido por el *compliance officer* y su equipo o por el Responsable del departamento de HR y sus miembros, dependiendo del contenido de la comunicación. Asimismo, cuando se produzca la intervención de cualquiera de los dos departamentos, estos estarán obligados a garantizar la más estricta confidencialidad con respecto a los datos y la información de los que tengan conocimiento a raíz de su labor de apoyo;
- si hay indicios racionales de la existencia de un ilícito penal, irregularidad, infracción y/o incumplimiento de la normativa vigente o de las normas y políticas internas de SCRM;
- si la comunicación recae en el ámbito de competencia de otra empresa del Grupo, en cuyo caso se derivará la comunicación a la responsable competente;
- si la comunicación contiene indicios de que está implicado un miembro del órgano de administración o el CEO, se transferirá el aviso al Delegado de *compliance* del Grupo; y/o
- si se trata de hechos que revisten indicios de delito y que requieren su comunicación inmediata al Ministerio Fiscal o a la Fiscalía Europea en caso de que los hechos afecten a los intereses financieros de la Unión Europea.

B) Las infracciones sujetas a la investigación que cumplan con los siguientes criterios deberán ser comunicadas al Delegado de *compliance* del Grupo:

Existe una afectación para el Grupo si es posible que:

- exista un delito de corrupción en el ejercicio del cargo (corrupción en relación con un funcionario público); o
- se haya cometido un delito de corrupción en el curso de la actividad empresarial con un beneficio prohibido superior a 1.000 euros (soborno y corrupción en relación con un empleado o agente de una empresa); o
- exista una participación/afectación en varias empresas o divisiones nacionales; o
- dentro de la empresa se vea afectado un órgano, miembro de la dirección, el *compliance officer* o Delegado de Protección de datos; o
- SCRM haya sufrido daños por un importe superior a 250.000 euros (por ejemplo, multas, daños y perjuicios, daños materiales, etc.); o
- se produzca un daño a la reputación del Grupo.

Existe un conflicto de intereses si:

- en el marco de la tramitación del aviso o del caso también se ven afectados los intereses privados del *compliance officer* o el CEO; o
- el propio Responsable del Sistema y de *compliance* Penal se ve afectado por el caso.

C) Si la comunicación no entra dentro del alcance del Sistema y/o no está debidamente fundada, o no cumple, en general, con los requisitos de veracidad, claridad y buena fe, se ordenará su archivo inmediato.

El Responsable del Sistema informará, en cualquier caso, a la Persona Interesada de la decisión adoptada sobre la admisión o archivo de la comunicación, así como de las razones que motivan una u otra decisión, en el plazo máximo de 3 meses desde el acuse de recibo o, si no se hubiese producido dicho acuse de recibo, desde el vencimiento del plazo de 7 días desde la recepción de la comunicación. Todo ello salvo en los casos de especial complejidad que requieran más tiempo para la investigación, donde el plazo de 3 meses podrá extenderse hasta un máximo de otros 3 meses adicionales.

(Es oportuno revisar el protocolo anti-acoso y de rechazo de cualquier tipo de violencia en el trabajo en el portal de HR para consultar procedimiento y plazos concretos relacionados con esta materia).

4.4 Apertura de expediente

Si, tras el análisis de los hechos contenidos en la comunicación, el Responsable del Sistema considera que concurren en el caso indicios razonables de la existencia de un incumplimiento, acordará la apertura del expediente y el inicio de la correspondiente investigación interna.

Paralelamente a la apertura del expediente el Responsable del Sistema podrá adoptar medidas de seguridad cautelares a fin de evitar poner en riesgo el desarrollo de la investigación o que sean precisas para proteger a las Personas Interesadas, testigos y/o las terceras partes que hayan podido resultar perjudicadas.

Siempre que sea necesario para poder llevar a cabo dichas acciones, el Responsable del Sistema podrá apoyarse en los departamentos o áreas funcionales que correspondan, especialmente en el departamento de *compliance* y HR y siempre respetando la confidencialidad.

4.5 Investigación interna de la comunicación

El responsable para llevar a cabo las investigaciones es el Responsable del Sistema.

Se establece un plazo máximo para la realización de la investigación de cualquier tipo de infracción (menor o no menor) de 3 meses a contar desde la remisión del acuse de recibo o, si no se hubiese producido dicho acuse de recibo, desde el vencimiento del plazo de 7 días desde la recepción de la comunicación. En los casos de especial complejidad que requieran más tiempo para su tramitación, el plazo de 3 meses podrá extenderse hasta un máximo de otros 3 meses adicionales. Para los supuestos en que la comunicación verse sobre materias protegidas por el Protocolo anti- acoso y de rechazo de cualquier tipo de violencia en el trabajo deberá estarse a lo dispuesto en el apartado 4.11 del referido Protocolo.

Las personas implicadas en la investigación del expediente deberán suscribir compromisos de confidencialidad, así como una declaración de ausencia de conflicto de interés.

Se garantizará la colaboración de las personas empleadas de la Organización, cuyos conocimientos o implicación se requieran para la realización de dicha investigación, garantizando siempre la confidencialidad del expediente.

En caso de que la comunicación esté ligada a incumplimientos especialmente graves o cuando las circunstancias del caso así lo requieran, el Responsable del Sistema adoptará las medidas oportunas para garantizar, en todo momento, la objetividad de la investigación.

Sin perjuicio de lo anterior, el Responsable del Sistema podrá externalizar la instrucción de la investigación en los casos en que, dada la naturaleza, gravedad, complejidad o partes implicadas en los hechos, resulte aconsejable para una adecuada resolución del expediente al que ha dado lugar la comunicación.

En los supuestos en que sea preciso interrogar directamente a las Personas Susceptibles de ser Denunciadas, en el marco de la investigación interna, se cumplirán las obligaciones de información sobre protección de datos. No está permitido informar a otras personas (en particular, al superior directo, al superior disciplinario, al jefe de departamento), de la necesidad de entrevistar a las Personas Susceptibles de ser Denunciadas. Todo ello a razón de la garantía de confidencialidad la presunción de inocencia de estas.

En caso de que sea preciso el Responsable del Sistema involucrará a las autoridades policiales, judiciales, administrativas y aduaneras cuando no sea posible aclarar los hechos a través de medidas internas;

4.6 Información y trámite de audiencia

Las Personas Susceptibles de ser Denunciadas cuyas conductas hubieran sido identificadas como presuntamente irregulares en la comunicación, serán informadas por el Responsable del Sistema de esta circunstancia y del tratamiento de sus datos, en cuanto la situación del procedimiento lo permita. Concretamente, las Personas Susceptibles de ser Denunciadas, contra las que se haya dirigido la comunicación, tendrán derecho a tener conocimiento de los hechos relatados de manera sucinta, pero en ningún caso se les revelará la identidad de la Persona Interesada.

La Persona Susceptible de ser Denunciada, contra la que se haya dirigido la comunicación tiene garantizado el derecho de ser oído en cualquier momento según lo establecido en el Art. 9.2. f) de la Ley de Protección de Informantes. Además, a través del trámite de audiencia, el Responsable del Sistema garantizará el derecho de la Persona Interesada y de la Persona Susceptible de ser Denunciada a plantear por escrito los argumentos, alegaciones y pruebas que a su derecho convengan.

Asimismo, siempre se garantizará a las Personas Susceptibles de ser Denunciadas el derecho de contradicción, el respeto a la presunción de inocencia y al honor.

4.7 Conclusiones y resolución de la investigación

4.7.1 El informe de la investigación

Si la investigación se lleva a cabo por parte de una persona externa o un departamento interno asignados para ello, estos deberán elaborar y remitir al Responsable del Sistema un informe de investigación que comprenderá un resumen de las investigaciones realizadas, las pruebas obtenidas y la conclusión del proceso de investigación. Dicho informe deberá remitirse al Responsable del Sistema en un plazo máximo de 15 días desde que finalizó la investigación de los hechos y, en cualquier caso, antes de los 3 meses establecidos para la investigación o, en su caso, de la finalización de la correspondiente prórroga prevista para los casos de especial complejidad. De nuevo, para el supuesto de que la investigación que verse sobre materias protegidas por el Protocolo anti-acoso y de rechazo de cualquier tipo de violencia en el trabajo deberá estarse a lo dispuesto en el apartado 4.11 del referido Protocolo.

A continuación, el Responsable del Sistema examinará el resultado de la investigación realizada.
En caso de existir uno de los incumplimientos descritos en la presente Política, el Responsable del Sistema proporcionará información ad hoc al superior jerárquico, al director correspondiente, al CEO y en su caso al superior directo (técnico) y al Responsable de *compliance* o Responsable de HR, con una recomendación. La información podrá incluir las medidas de seguridad provisionales aplicadas y los hechos completos del caso con el nombre de la Persona Susceptible de ser Denunciada contra la que se ha dirigido la investigación.

Si no existe violación de cumplimiento, el Responsable del Sistema enviará información ad hoc al CEO con una recomendación. En ambos casos la Persona Interesada únicamente podrá identificarse si nos encontramos ante un incumplimiento que queda al margen de las infracciones de Derecho de la Unión Europea e infracciones penales o administrativas graves o muy graves que se describen en el apartado 2.3 de la presente Política y si es necesario para la evaluación de los hechos.

Además, el Responsable del Sistema elaborará y presentará informe *ad hoc* al Delegado de *compliance* del Grupo Schwarz si hay algún asunto de relevancia para el Grupo. El informe deberá incluir una descripción completa de los hechos con el nombre de la Persona Susceptible de ser Denunciada contra la que se ha dirigido la Investigación. El nombre de la Persona Interesada solo se proporcionará si nos encontramos ante un incumplimiento que queda al margen de las infracciones de Derecho de la Unión Europea e infracciones penales o administrativas graves o muy graves que se describen en el apartado 2.3 de la presente política y si es necesario para la evaluación de los hechos.

Basándose en el informe de investigación, el Responsable del Sistema resolverá:

- Archivar la comunicación: Se procederá al archivo de la comunicación recibida en caso de que en virtud de la información y documentación remitida no resulte razonablemente acreditada la comisión de un incumplimiento, infracción o irregularidad. Así mismo, tampoco se tramitará expediente en caso de que la información aportada carezca de fundamento o verosimilitud.

- Tramitar un expediente sancionador: En caso de que, de la información y evidencias obtenidas en la comunicación o documento adjuntos a la misma, se desprendan evidencias de la comisión de un incumplimiento, infracción o irregularidad en el seno de la Organización, se procederá a iniciar un expediente sancionador. En el expediente sancionador se determinarán las posibles responsabilidades y se podrán adoptar las siguientes medidas:

  (I) La corrección inmediata del incumplimiento y la adopción de las medidas de reparación del derecho vulnerado y de prevención de futuros incumplimientos que, en su caso, correspondan.

  (II) Las medidas disciplinarias, que podrán ir desde el simple apercibimiento o amonestación, hasta el despido; En este caso será involucrado el departamento de HR.

  (III) El traslado al departamento competente de la resolución para la adopción, y en todo caso aplicación, de las medidas de remediación que, en su caso, resulten necesarias, de las que se dará oportuna cuenta al Responsable del Sistema y de *compliance* Penal y al *compliance officer*.

En el supuesto de que resulte necesaria la adopción de medidas deberá procederse a la implementación de las mismas en un plazo de 20 días a contar desde la emisión del informe de investigación.

- Reclamar una indemnización por daños y perjuicios: Si se ha comprobado que ha lugar a reclamaciones por daños y perjuicios (por ejemplo, contra la Persona Susceptible de ser Denunciada contra la que se ha dirigido la investigación, otros empleados o socios comerciales), el Responsable del Sistema en conjunto con *compliance officer* y CEO, el superior jerárquico decidirá si hacer valer o renunciar a dichas reclamaciones. El superior jerárquico involucrará en el proceso al área de HR en la medida de lo necesario;

- Denunciar los hechos a las autoridades competentes: En caso de que el *compliance officer* y el Responsable del Sistema consideren que la situación informada por la Persona Interesada pudiera ser constitutiva de un delito, tras el estudio de la información obtenida, emitirán informe dirigido al CEO para que este adopte la decisión correspondiente de interposición de denuncia ante las autoridades policiales y/o el órgano judicial competente.

El Responsable del Sistema únicamente comunicará el contenido de la resolución y el tipo de medidas que, en su caso, se establezcan, al responsable del departamento o área correspondiente, a las Personas Interesadas y a las Personas Susceptibles de ser Denunciadas contra las que se ha dirigido la investigación y, cuando proceda la adopción de medidas disciplinarias, se informará también al departamento de HR, para la planificación y ejecución de las mismas.

El Responsable del Sistema previo a la elaboración del informe final registrará las medidas derivadas y verificará la ampliación del periodo del borrado estándar. Dicho informe contendrá los resultados de la investigación interna y las medidas adoptadas.

Tras la preparación del informe final, se proporcionará información ad hoc al CEO y al director responsable. La información podrá incluir los hechos completos con el nombre de la Persona Susceptible de ser Denunciada contra la que se ha dirigido la investigación. De la Persona Interesada solo se dará el nombre si nos encontramos ante un incumplimiento que queda al margen de las infracciones de Derecho de la Unión Europea e infracciones penales o administrativas graves o muy graves que se describen en el apartado 2.3 de la presente Política y si es necesario para la evaluación de los hechos. En caso de acciones u omisiones cometidas o que estén en proceso de cometerse por alguna de las Personas Susceptibles de ser Denunciadas en nombre o por cuenta de SCRM que puedan constituir un incumplimiento de la normativa interna de SCRM y/o del Grupo, se enviará información adicional ad hoc sobre las medidas adoptadas a los responsables de los equipos, sin referencia a las personas.

En casos que afecten especialmente al Grupo, se enviará una copia del informe final al Delegado de *compliance* del Grupo Schwarz, independiente de si se ha determinado o no la existencia de una infracción. Finalmente, tras la expiración del periodo de borrado se realizará la eliminación oportuna de los datos personales. Se presentará en el expediente del caso una versión anónima del informe final que incluirá anexos anónimos (por ejemplo, el informe de investigación). Según el principio de anonimización se eliminarán los nombres concretos de las personas. En casos excepcionales se utilizarán o conservarán las designaciones de funciones.

5 CONSERVACIÓN, CUSTODIA Y ARCHIVO DE LA INFORMACIÓN

El Responsable del Sistema mantendrá un registro actualizado de todas las comunicaciones recibidas, de las aperturas de los expedientes, así como, en su caso, de las investigaciones internas llevadas a cabo y de las medidas adoptadas, durante los plazos que, de acuerdo con la normativa aplicable, se encuentren legalmente permitidos en cada caso.

Los datos de carácter personal obtenidos en el marco de la investigación interna serán suprimidos cuando dejen de ser necesarios y pertinentes y, en todo caso, en el plazo máximo de 3 meses desde que se reciba la comunicación, salvo que la investigación siga en curso.

Si la comunicación recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de estos.

Si se acredita 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.

Los datos personales relativos a comunicaciones que no entren dentro del alcance del Sistema, que no sean necesarios para el desarrollo de la investigación y/o no sean objeto de investigación, se suprimirán sin demora, con excepción de su puesta a disposición de las administraciones públicas u órganos jurisdiccionales, en caso de que pudieran ser necesarios para la atención de posibles responsabilidades durante los periodos de prescripción correspondientes. Tras ello, se procederá a la supresión física de los datos.

6 PROTECCIÓN DE DATOS PERSONALES

6.1 Categorías de datos tratados

El uso del Sistema es voluntario. El tipo de datos personales que serán tratados dependerá de la información que la Persona Interesada proporcione en el marco de su comunicación y de la información que sea recabada a lo largo de la eventual investigación que pueda iniciarse.
Por regla general, se tratarán los datos siguientes:

- Datos identificativos, tales como nombre y apellidos, datos de contacto y los relativos a la condición del empleado (por ejemplo, el número de empleado) de la Persona Interesada, de la Persona Susceptible de ser Denunciada o de cualquier otro perjudicado;
- Si la Persona Interesada es empleada de SCRM, siempre que lo desee comunicar el mismo;
- Relación con SCRM;
- Incumplimientos comunicados;
- Documentación que pruebe los incumplimientos denunciados.

6.2 Finalidad del tratamiento de datos y base jurídica

Los datos personales serán tratados a los efectos de detectar, investigar y evaluar legalmente las sospechas de las infracciones comunicadas.

Los hechos o actuaciones comunicadas necesariamente deberán tener una vinculación efectiva con la relación laboral, comercial o profesional que vincule a las Personas Susceptibles de ser Denunciadas directamente con SCRM.

Por otro lado, podrá utilizarse el SII cuando se desee plantear preguntas concretas en materia de cumplimiento normativo que se quieran aclarar con los empleados del Departamento de Legal y *compliance*.

La base jurídica de los referidos tratamientos es el cumplimiento de las obligaciones legales (art. 6.1 c) RGPD, art. 8.1. LOPDGDD y art. 11 de Ley Orgánica 7/2021, de 26 de mayo) de disponer de un sistema interno de información de acuerdo con la Ley de Protección de Informante. Para el tratamiento de datos personales derivado de una revelación pública la base de legitimación será la existencia de un interés público en prevenir y actuar frente a infracciones de la legislación aplicable (art. 6.1 e) RGPD y art. 8.2. LOPDGDD) y en la medida en la que se traten categorías especiales de datos personales también de acuerdo con el art. 9.2. g) RGPD.

6.3 Destinatarios de los datos personales

Es posible que para cumplir las finalidades del tratamiento arriba referidas se tenga que dar acceso / facilitar los datos personales a otros departamentos, áreas o bien a sociedades del Grupo, siempre que ello sea necesario para la aclaración de los hechos o la aplicación de las medidas de actuación o procedimientos sancionadores o penales como la consecuencia de investigación. Asimismo, se concederá el acceso a los datos al Abogado de confianza u otros prestadores de servicio, tales como asesores y colaboradores externos que presten soporte en la gestión o investigación de la comunicación. Por lo tanto, el acceso a los datos personales contenidos en el Sistema quedará limitado dentro del ámbito de sus competencias y funciones, exclusivamente a:

- El Responsable del Sistema y a quien lo gestione directamente, en el caso de SCRM, el departamento de *compliance* o HR.
- El responsable del departamento Legal, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Los encargados del tratamiento que eventualmente se designen.
- El delegado de protección de datos.

Igualmente, los datos podrán ser objeto de cesión a los jueces y tribunales, al Ministerio Fiscal o a las administraciones públicas competentes como consecuencia de la investigación que se pueda poner en marcha.

Tan pronto como esta información deje de poner en peligro el seguimiento de la comunicación SCRM tendrá la obligación legal a informar a las Personas Susceptibles de ser Denunciadas, de que se ha recibido una comunicación que les incumbe. La identidad de la Persona Interesada no se hará pública, siempre que ello sea jurídicamente admisible.

6.4 Transferencias Internacionales

Lo datos personales solo se transmiten a destinatarios fuera del Espacio Económico Europeo (EEE) si la Comisión de la Unión Europea ha otorgado al país tercero un grado razonable de protección, si se ha acordado con el destinatario de los datos un grado razonable de protección (mediante cláusulas contractuales estándares de la UE), o si las Personas Interesadas, Susceptibles de ser Denunciadas o terceras partes han dado su consentimiento a dicha transmisión.

6.5 Derechos

Las Personas Interesadas, Personas Susceptibles de ser Denunciadas y cualquier tercero cuyos datos hayan sido facilitados en el marco de la comunicación y/o investigación pueden ejercitar los siguientes derechos:

- Derecho a obtener, a petición y gratuitamente, información sobre sus datos personales almacenados;
- Siempre que se cumplan los requisitos legales, tienen derecho a rectificación, supresión y limitación del tratamiento;
- Si ellos mismos han proporcionado los datos tratados, les corresponde el derecho a la portabilidad de los datos;
- Derecho a revocar el consentimiento con efectos futuros, si la base legal del tratamiento de datos es una declaración de consentimiento;
- Derecho de oposición si el tratamiento de datos se basa en el artículo 6.1 e) o f) RGPD. En case de la oposición, el tratamiento ya no se llevará a cabo, a menos que SCRM pueda aducir razones imperiosas de interés general que justifiquen el tratamiento ulterior de los datos, a pesar de tal oposición.

Los referidos derechos podrán ejercitarse mediante el envío, a la atención del Delegado de Protección de Datos de un correo ordinario a domicilio social de SCRM o de un correo electrónico a la siguiente dirección: dataprotection@scrm.lidl, identificando el derecho que desean ejercitar.
Asimismo, tendrán el derecho a presentar una reclamación ante la Agencia Española de protección de Datos o, en su caso, ante la autoridad competente.

7 VIGENCIA

La presente Política será vigente desde el momento de su aprobación por parte del comité de dirección de SCRM, siendo aplicable hasta el momento en el que se realice actualización o modificación si procediese en atención a la revisión del procedimiento.

APROBADO POR	VERSIÓN DEL DOCUMENTO	FIRMA	FECHA
	Versión 1		

***


LIDL
SCRM
INTERNATIONAL HUB