



12. PROTOCOLO DE PUESTA EN CONOCIMIENTO

Fecha y nº de versión	Persona responsable	Encargado de aprobación
27/11/2023. Versión 2ª	Órgano de Supervisión y Control	Consejo de Administración

1. INTRODUCCIÓN

La Sociedad Deportiva Eibar, S.A.D., (en adelante también, "el Club" o "el Eibar") está comprometida con el cumplimiento de la legislación nacional e internacional que regula todos los aspectos de su actividad.

En virtud de dicho compromiso, el órgano de administración del Club, en cumplimiento de sus responsabilidades, ha promovido la redacción y la aplicación de este Protocolo de Puesta en Conocimiento (en adelante, "el Protocolo") que regula el "sistema interno de información del Club" conocido como Canal Ético.

Este Protocolo establece una serie de reglas y pautas de actuación en relación con el procedimiento para tramitar y resolver cualquier denuncia recibida sobre posibles incumplimientos al Manual de Cumplimiento Normativo o a la legislación en vigor.

2. OBJETO Y FINALIDAD

La finalidad del presente Protocolo no es otra que crear un cauce mediante el cual, cualquier persona, pueda poner en conocimiento del Club cualquier incumplimiento o sospecha de incumplimiento de la que se tenga conocimiento, tanto en relación con los Sistemas de Gestión de Compliance Penal y Antisoborno implantados en la entidad, como con cualquier otra materia que no estuviese prevista en los mismos; con el fin de que el Club pueda dar trámite y resolver dichas denuncias de conformidad con la legislación vigente en cada momento.

3. ÁMBITO DE APLICACIÓN

El presente Protocolo será de aplicación a todas las personas relacionadas con el Club. Esto es, a miembros del Consejo de Administración, directivos, jugadores de los distintos equipos del Club, miembros de los diferentes cuerpos técnicos, personal médico y de fisioterapia y otros empleados (en adelante, "Personas Vinculadas") así como a cualquier persona, física o jurídica, que mantenga algún tipo de relación con la Sociedad Deportiva Eibar, S.A.D. y que, en el desarrollo de su actividad, puedan tener conocimiento de la existencia de algún incumplimiento normativo. Asimismo, este Protocolo resulta de aplicación a todas aquellas personas que comuniquen cualquier presunto incumplimiento a través de las vías habilitadas que se exponen en el presente Protocolo.

4. PRINCIPIOS DE ACTUACIÓN

El procedimiento de actuación se regirá por los siguientes principios y garantías, que deberán ser observados en todo momento:

- Garantía de confidencialidad de la identidad del informante, del investigado y de cualquier otra persona o tercero afectado, así como del tratamiento de la información y de la investigación realizada.

- Protección de la intimidad y dignidad de las personas implicadas.
- Prioridad y tramitación urgente, atendiendo a la naturaleza de la denuncia.
- Investigación exhaustiva de los hechos, llevada a cabo por profesionales especializados, en caso de que fuese necesario.
- Garantía del principio de presunción de inocencia y del derecho de defensa de las partes afectadas.
- Garantías de actuación adoptando las medidas necesarias, incluidas las de carácter disciplinario.
- Indemnidad frente a represalias contra denunciadores de buena fe.
- Posibilidad de presentación de denuncias anónimas.

5. CONTROL, REVISIÓN Y FORMACIÓN

El Órgano de Supervisión y Control será el encargado de controlar internamente que lo contenido del presente Protocolo se está aplicando de manera correcta.

Con independencia de que el Órgano de Supervisión y Control sea el encargado de velar internamente por la aplicación del contenido de este Protocolo, su contenido es de obligado conocimiento, aplicación y cumplimiento por parte de todas las Personas Vinculadas al Club, por lo que estará a disposición de todos estos para su consulta.

I. Procedimiento

La Sociedad Deportiva Eibar, S.A.D. ha creado la figura del Órgano de Supervisión y Control que cuenta, como responsable del canal ético, entre sus funciones con la de canalizar las quejas y denuncias que se produzcan por cualquier tipo de incumplimiento normativo o de lo establecido en el Manual de Cumplimiento Normativo del Club y velar en general por la efectiva implantación y funcionamiento del mismo.

a) Inicio: Presentación de la denuncia.

En un primer momento, el interesado podrá poner en conocimiento del Órgano de Supervisión y Control de forma confidencial y, en su caso, anónima, el objeto de su denuncia por escrito (incluso anónimamente) o de forma verbal.

El cauce para la presentación de denuncias será a través de la plataforma tecnológica [Whistleblower Software](#), plataforma que permite la presentación de denuncias por distintas vías:

1. Por escrito sin anonimato (en cualquier caso, siempre se asegura la absoluta confidencialidad de los datos de las personas involucradas – denunciante, denunciado, testigos y cualquier otro posible involucrado-).
2. Por escrito con anonimato. En caso de que el denunciante así lo prefiera, podrá presentar su denuncia con carácter anónimo seleccionando la casilla correspondiente en la plataforma tecnológica del canal de denuncias. En este caso, el denunciante, deberá guardar la contraseña que le proporciona la plataforma para poder hacer el oportuno seguimiento de su denuncia y mantener comunicación bidireccional con el gesto del asunto.
3. De forma verbal sin anonimato. La plataforma tecnológica tiene habilitada la posibilidad de informar oralmente, mediante grabación de audio y en un formato seguro, duradero y accesible. En caso de que el denunciante no tenga intención de preservar el anonimato, una vez realizada su grabación de audio, no deberá marcar la opción habilitada de distorsión de audio.
4. De forma verbal con anonimato. La plataforma tecnológica tiene habilitada la posibilidad de informar oralmente, mediante grabación de audio y en un formato seguro, duradero y accesible. En caso de que el denunciante tenga intención de preservar el anonimato, una vez realizada su grabación de audio, deberá marcar la opción habilitada de distorsión de audio y, si lo desea, eliminar los metadatos del archivo de audio.

En todos los casos anteriormente expresados, se dará acuse de recibo al denunciante en el plazo máximo de siete (7) días desde la recepción de la misma.

De igual forma, se prevé la posibilidad de que el denunciante solicite una reunión presencial con el Órgano de Supervisión y Control como responsable del Canal Ético. En este caso, la conversación será grabada en un formato seguro, duradero y accesible o se recogerá el contenido de la reunión por escrito mediante una transcripción completa y exacta de la conversación que será firmada tanto por el denunciante como por el/los miembro/s del Órgano de Supervisión y Control que mantengan la reunión presencial con el denunciante. Los datos de los miembros del Órgano de Supervisión y Control son:

- Vocal interno: doña Elisa Mangado.
Email: elisa.mangado@sdeibar.com
- Vocal asesor externo : Eversheds Sutherland, representada por don Fabio Pérez-Bryam
Email : fperezbryan@eversheds-sutherland.es

El canal interno descrito en este procedimiento será el preferente para informar. En caso de que perciba riesgo de represalias por el uso de canal interno, el denunciante podrá comunicar su denuncia a través de distintos canales externos de información:

- Unión Europea: <https://commission.europa.eu/about-european-commission/contact/problems-and-complaints_en>.

- Autoridad Independiente de Protección del Informante.¹
- En su caso, la Autoridad autonómica competente.²

La información que se proporcione en relación con el incumplimiento observado podría afectar a otras personas, por lo que el denunciante interesado deberá asegurarse de que la información es correcta y deberá actuar con la máxima confidencialidad.

b) Investigación de la denuncia

El Órgano de Supervisión y Control tendrá las facultades suficientes para dirigirse a cualquier persona del Club, con independencia del nivel jerárquico de la misma, para obtener la información y datos necesarios para el correcto desarrollo de la investigación.

Asimismo, durante el periodo de investigación, el Órgano de Supervisión y Control y/o los profesionales especializados encargados de la investigación, practicarán las pruebas necesarias para una eficaz investigación de los hechos (entrevistas a implicados, solicitud de documentos, etc.) garantizando el máximo respeto a la presunción de inocencia, al derecho de defensa y al honor de las personas afectadas

En todo caso, el proceso formal de investigación no durará más de tres (3) meses, desde la recepción de la comunicación o denuncia, salvo en aquellos casos de especial complejidad que requieran una ampliación de plazo, en cuyo caso podrá extenderse hasta un máximo improrrogable de otros tres (3) meses adicionales.

Adicionalmente, cuando los hechos pudieran ser constitutivos de delito, el Órgano de Supervisión y Control deberá remitir la información al Ministerio Fiscal.

c) Medidas correctoras: informe emitido por el Órgano de Supervisión y Control

Una vez finalizado el proceso de investigación, el Órgano de Supervisión y Control, dentro del plazo referenciado en el apartado anterior, emitirá un informe por escrito en el que (i) se identificarán los hechos denunciados y el proceso de investigación seguido (ii) se establecerán las medidas correctoras o disciplinarias oportunas, en caso de que tras el proceso de investigación se haya llegado a la conclusión de que efectivamente, se ha producido un incumplimiento normativo susceptible de ser corregido o sancionado; o por el contrario (iii) se ordenará el archivo de la denuncia al comprobarse que no ha existido incumplimiento normativo alguno.

d) Disposiciones adicionales

¹ A fecha del presente protocolo no se ha creado la Autoridad Independiente de Protección al Informante.

² A fecha del presente protocolo el País Vasco no ha designado una Autoridad autonómica competente ni la Diputación Foral de Gipuzkoa.

Medidas cautelares: durante la tramitación del procedimiento, el Órgano de Supervisión y Control adoptará las medidas que sean necesarias, conducentes al cese inmediato del incumplimiento que se estuviese produciendo, de haberse probado el mismo o aquellas necesarias para llevar a cabo de forma efectiva la investigación.

Asistencia a las partes: durante el desarrollo del proceso de investigación, las partes implicadas podrán ser asistidas por una persona de confianza, la cual deberá guardar confidencialidad sobre la información que conozca por razón del mismo.

Prohibición de represalias: se prohíben expresamente los actos constitutivos de represalias, incluidas las amenazas de represalias contra las personas que efectúen una denuncia, comparezcan como testigos o ayuden o participen en una investigación sobre cualquier incumplimiento normativo.

Denuncias falsas: quedan prohibidas expresamente todas aquellas denuncias que no se ajusten a la realidad, o que el Responsable de Cumplimiento las haya reputado como falsas, pudiendo por ello, establecer la respectiva sanción a aquella Persona Vinculada con el Eibar que formule una denuncia falsa o inveraz.

6. GARANTÍAS EN RELACIÓN A PROTECCIÓN DE DATOS

A continuación, se describen las consideraciones en materia de protección de datos según las disposiciones legales siguientes:

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD),
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD),
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Licitud del tratamiento

Cuando es la implantación del Sistema de Información sea obligatorio, se presumirá lícito en cumplimiento de una obligación legal aplicable³. De no establecerse como obligatorio o mediante una revelación pública, el tratamiento de datos, estará amparado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable⁴.

Del mismo modo, en los casos de **comunicación de datos dentro de la organización** (siempre de forma confidencial y a las personas autorizadas), se entenderá lícita esta comunicación en base a criterios normativos

Cuando se produzcan tratamientos de datos de **categoría especial por razones de un interés público esencial**, será lícito este tratamiento en virtud del artículo 9.2.g) RGPD.

³ Artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

⁴ Artículo 6.1 e) RGPD.

Transparencia e Información

Los informantes que utilicen el canal, deberán ser informados de acuerdo con el artículo 13 RGPD y el artículo 11 LOPDGDD.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante.

Asimismo, los **empleados y terceros** deberán ser informados acerca del tratamiento de datos personales en el marco de los sistemas de información.

En el caso de los empleados, deberán haber sido informados previamente de la existencia de estos sistemas y del tratamiento de los datos que conlleva la formulación de una denuncia.

La información puede proporcionarse por varios cauces:

- Directamente en el contrato de trabajo.
- Individual o colectivamente al implementar o modificar el sistema.
- Mediante circulares informativas al personal y a su representación informando de la existencia y finalidad de un tratamiento de datos relacionado con estos buzones o sistemas de denuncias.

Derechos de los interesados

Los interesados podrán ejercitar sus derechos en materia de protección de datos. Sin embargo, en caso de que la persona a la que se refieran los hechos relatados ejerciese el **derecho de oposición**, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Acceso a los datos

El acceso a los datos contenidos en el sistema interno de información quedará limitado exclusivamente a:

- El Responsable del Sistema y a quien lo gestione directamente,
- El responsable de recursos humanos o el órgano competente debidamente designado, **sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador**,
- El responsable de los servicios jurídicos de la entidad u organismo, **si procediera la adopción de medidas legales** en relación con los hechos relatados en la comunicación,
- Los encargados del tratamiento (si existen para este procedimiento),
- El delegado de protección de datos (si se ha designado internamente).

El acceso a los datos por parte de personas distintas a las anteriores será válido sólo cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

Minimización de datos

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

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Datos especialmente protegidos

Si la información 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 los mismos.

Conservación de los datos

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos **tres meses** desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma **anonimizada**, sin que sea de aplicación la obligación de bloqueo de la normativa de protección de datos.

Confidencialidad

La identidad de las personas que denuncien no será revelada a terceras personas. Los sistemas de información, tanto internos como externos, no deberán obtener datos que permitan la identificación del informante.

Además, estos sistemas deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

La identidad del informante sólo 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. En estos casos, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

Registro de actividades de tratamiento

El tratamiento de datos personales realizado mediante el sistema interno de información requiere la creación de un registro de actividades de tratamiento. Éste deberá contener, al menos:

- los fines del tratamiento;

- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluidas las garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Análisis de riesgos

El tratamiento de datos personales realizado mediante el sistema interno de información requiere que se analicen las amenazas a las que puede verse expuesto en materia de protección de datos, a través de un análisis de riesgos.

7. RÉGIMEN SANCIONADOR

La realización de cualquier conducta que vaya en contra o que no cumpla con lo recogido en el presente Protocolo podrá tener consecuencias disciplinarias de conformidad a lo establecido, tanto en el Convenio Colectivo que sea de aplicación.