INTERNAL INFORMATION SYSTEM POLICY

DORNA GROUP
MARCH 2023

Index

1. Introduction....2
2. Purpose....2
3. Principles governing the internal information system and the internal reporting channel....3
4. Internal channels integrated into DORNA's information system....5
4.1. Presentation of communications....5
4.2. Internal reporting channel guarantees....6
4.2.1. Whistleblower guarantees....6
4.2.2. Guarantees of the person affected....6
5. Modification of the Internal Information System Policy....7
6. Approval and entry into force....7

1. Introduction

This **Policy is applicable** to the companies (i) **DORNA SPORTS, S.L.**, with registered office at Calle Príncipe de Vergara, nº 183, Madrid - P.C. 28002 and Tax Identification Code B- 84760800, (ii**)** **DORNA WORLDWIDE, S.L.U.**, with registered office at Calle Príncipe de Vergara, nº 183 de Madrid - P.C. 28002 and Tax Identification Code B-82846320 and (iii) **INTERNATIONAL EVENTS SERVICES, S.L.U.**, with registered office at Calle Príncipe de Vergara nº 183 de Madrid - P.C. 28002 and Tax Identification Code B- 82626144 (hereinafter, "**DORNA**").

Due to the entry into force of the Criminal Code reforms that constitute the legal framework for the criminal liability of legal persons in our legal system, introduced by Organic Law 5/2010 of June 22, Organic Law 1/2015 of March 30 and the recent Organic Law 1/2019 of February 20, 2009, companies have found it necessary to implement effective regulatory compliance systems in order to detect and ultimately prevent the commission of crimes in the performance of their usual activities.

In this context, the transposition of Directive 2019/1937 of the European Parliament and of the Council of October 23rd, 2019, on the protection of persons reporting breaches of Union law has taken place.

The approval of Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption, stipulates the obligation of companies that meet the conditions set forth to have an internal information system that allows them to report the actions or omissions established in the aforementioned legal text.

Additionally, this document complies with the provisions of clause 9.1.3 "Sources of opinion on Compliance performance" and 10.1.2 "Information Escalation" of ISO 19600:2015 and with the provisions of section 8.7. "Communication of non-compliances and irregularities" and 8.8. "Investigation of non-compliances and irregularities of the UNE 19601:2017 standard".

In the same way, the present Policy is based on the latest regulatory reforms operated by Organic Law 3/2018, of December 5th, 2018, on Personal Data Protection and guarantee of digital rights.

2. Purpose

The purpose of this Internal Information System Policy is to set forth the underlying principles regarding the internal information system and the guarantees for the protection of the whistleblower and the person affected by the communication.

The content of this Policy is mandatory for all members, employees and professionals of the companies that make up **DORNA** for whose purpose it is made available.

In addition, any person working for or under the supervision and direction of contractors, subcontractors, and suppliers of **DORNA** will have the possibility to report violations in a work or professional context.

DORNA employees and members will have the obligation to use the internal reporting channels made available to them to bring to the attention of the entity any breach of both the law and its internal regulations of which they may become aware.

Therefore, it could be said that the purpose of this Internal Information System Policy is to complete and adapt **DORNA's** internal policy procedures on communications and, ultimately, to improve the management system implemented at **DORNA**, in accordance with the commitment to the continuous improvement of the compliance function demonstrated by the company.

In this sense, **DORNA's** Internal Information System Policy is largely related to the Management of Communications Received Procedure, which establishes the mechanisms for the management and resolution of the communication made by the whistleblower.

For the purposes of this Policy, the following, among others, shall be considered as aspects susceptible to communication:

- Harassment, hostile or offensive conducts;
- Actions related to possible irregularities in the relationship with suppliers and/or purchases; Actions related to public and private corruption;
- Misappropriation and Diversion of Resources;
- Money Laundering;
- Misappropriation and Diversion of Resources;
- Accounting Irregularities and Inaccuracies;
- Conflict of Interest;
- Improper commitments with third parties;
- Falsification of documents, contracts, reports or records; Violation of employee rights, breaches of the applicable collective bargaining agreement;
- Violations of Information Security;
- Any behaviour involving improper conduct and irregularities which are contrary to values and principles that govern **DORNA**;
- And, in short, any behaviour that could contravene the applicable regulations, the Code of Conduct or **DORNA's** internal policies and procedures.

3. Principles governing the internal information system and the internal reporting channel

This type of procedure entails a high degree of responsibility for the person submitting the communication, as well as the risk of stigmatization and humiliation of persons within the organization to which he or she belongs. For this reason, the internal reporting system within **DORNA's** crime prevention program is based on the following principles:

a) Principle of Independence:

The procedures to which the different communications give rise shall be governed with the utmost objectivity and independence, establishing the corresponding mechanisms in order to avoid the concurrence of possible conflicts of interest.

b) Principle of Tolerance and Respect:

As a manifestation of the maximum rejection by **DORNA** to all those behaviours that are contrary to its principles and to the law in force, the obligation to communicate the knowledge of those to all members of the entity is imposed.

c) Principle of Confidentiality:

DORNA guarantees the utmost confidentiality of the communications received and the data contained within them.

It is specifically forbidden for the personal data contained in the communication to be known by any person at **DORNA** who (i) is not in charge of the management of the communication or (ii) is responsible for the application of the measures whose execution corresponds once the investigation has been completed.

The foregoing does not affect the data that must be disclosed to the authorities in the event that the nature of the facts or the existence of any procedure -both judicial or before the administration- that requires it.

Thus, the confidentiality of the whistleblower identity and of any third party mentioned in the communication, the actions carried out in the management and processing and the protection of data preventing access by unauthorized personnel is guaranteed.

d) Principle of Objectivity and Honesty:

The actions that mandate the management of communications procedure received shall in all cases be governed by the principles of absolute objectivity and utmost honesty.

e) Prohibition of Retaliation:

It is absolutely forbidden to take any action against any person who uses the internal reporting channels that involves retaliation or any negative consequence on the occasion of having made a communication in a proper manner and subject to the conditions of use of the internal reporting channel.

The foregoing is without prejudice to the adoption of appropriate measures when the internal investigation unequivocally shows that the communication is false or malicious.

In the event that it is determined that the accusations described in the communication are false or malicious to the extent that they have been made deliberately with knowledge of their falsity or recklessly, they will be considered a serious breach of this procedure.

On this basis, **DORNA** shall be entitled, in accordance with the Workers' Statute and the applicable collective agreement in the case of workers and the contracts signed in the case of professionals, to carry out any of the actions listed in Section 8 of the Management of Communications Received Procedure.

4. Internal channels integrated into DORNA's information system

The internal information system implemented by **DORNA** is an essential element within the organization's crime prevention management system, and must therefore be considered, respected and supported by all members of the company.

Also, the configuration of the internal reporting system is in line with the legal requirements established in Law 2/2023. It also complies with the recommendations made by the State Attorney General's Office in its Circular 1/2016. From this text it can be concluded that greater efficiency is obtained when the functions related to the management of the internal reporting channel are performed by outsourcing. Specifically, it alludes to the fact that they will be more used and effective when they are managed by an external company, since they guarantee higher levels of independence and confidentiality.

That is why **DORNA** has adopted an internal reporting channel managed by ECIJA as its external manager. More specifically, it is carried out through an IT tool -Whistle B, also an external third party- in order to (i) guarantee the requirement of effectiveness of the organization and management models in the field of Criminal Risk Prevention; (ii) to reinforce the surveillance and control measures suitable for the prevention of the commission of criminal activities within the company, all as established in the current Article 31 bis of the Criminal Code, introduced by the reform operated by Organic Law 1/2015, of March 30, which amends Organic Law 10/1995, of November 23, 1995, of the Criminal Code; and (iii) to comply with the obligations established by Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption.

Furthermore, together with the aforementioned internal reporting channel, there is the possibility, at the whistleblower request, of submitting a communication by means of a face-to-face or telematic meeting within a maximum period of seven (7) days, which is established in the internal information system.

When the communication by means of a face-to-face or telematic meeting is made verbally, it shall be documented by recording the conversation in a secure, durable and accessible format, or through a complete and accurate transcription of the conversation made by the personnel responsible.

4.1. Presentation of communications

In order to make it easier for members of the company and its stakeholders to report any conduct contrary to the Code of Ethics and the management system, **DORNA** has implemented an internal reporting channel that is managed through an external tool and is configured as follows:

i. **External Software:** WhistleB (external Swedish software with the highest levels of anonymity guarantees and whistleblower protection), which is constituted as a measure to ensure the guarantees of whistleblower protection.
ii. **Access method:** https://report.whistleb.com/dorna, which can be accessed from any device with internet connection.
iii. **External manager** (efficiency standard according to Circular 1/2016 of the State Attorney General's Office): ECIJA. Guarantees of autonomy and confidentiality.

Additionally, there is the possibility, at the whistleblower request, of submitting a communication by means of a face-to-face or telematic meeting within a maximum period of seven (7) days.

Communications submitted by means of a face-to-face or telematic meeting will receive the same consideration and procedure once they have been received as those submitted through the internal reporting channel.

Finally, it is necessary to point out that any individual may report to the Independent Whistleblower Protection Authority or to the corresponding regional authorities or bodies, the commission of any actions or omissions included in the scope of application of this law, either directly or after communication through the corresponding internal channel.

4.2. Internal reporting channel guarantees

4.2.1. Whistleblower guarantees

The internal reporting channel - as a channel existing in **DORNA's** internal information system - has the necessary guarantees to maintain the security of communications with the manager of the communication and the required confidentiality.

Once the communication is received by ECIJA, an examination of impartiality and absence of possible conflicts of interest will take place from the very beginning to ensure that the communication is investigated by an impartial person in the matter.

Once the impartiality and absence of conflict of interest with respect to **DORNA's** Compliance Officer has been determined, **DORNA's** Compliance Officer will be informed of the communication received and the communication will be classified so that, once the likelihood of it being a clearly false and/or malicious communication has been ruled out, the appropriate investigative actions will be carried out.

The investigation of the facts contained in the communications will be managed internally, corresponding to **DORNA's** Compliance Officer, with the support of ECIJA and the corresponding department according to the type of communication and the facts reported, the internal investigation procedure (after verification by ECIJA of the absence of conflict of interest as provided in the preceding paragraphs).

The people in charge of the management of the communication received shall be aware of the content of each of the communications and shall treat them with due diligence, always safeguarding the identity of the whistleblower in those cases in which it has been disclosed.

The internal reporting channel shall be governed by the principle of maximum confidentiality, adopting all necessary measures to ensure that there are no reprisals against the whistleblower.

4.2.2. Guarantees of the person affected

People who have been affected by the submission of a communication through the internal reporting channel may never be penalized by a simple communication or notification to any of the aforementioned recipients, being necessary, in any case, that the veracity of the communication is previously verified and that the persons involved are given the opportunity to offer an explanation to the situation reported.

The people affected by the communication will be informed by ECIJA and/or by the Compliance Officer, as appropriate, as soon as possible and, at the latest, within one (1) month from the receipt of the communication.

In particular, the person affected by the communication will be informed of the following:

- Details of the body responsible for managing the internal reporting channel;
- The facts communicated;
- The person responsible for processing the communication;
- The following facts that may occur in the course of the investigation;
- The information concerning the processing of your personal data;.

As an exception, if there is a significant risk that the notification to the person affected by the communication may jeopardize the effectiveness of the investigation or collection of evidence, the notification shall not be made until such risk has ceased to exist. The reasons that lead to the existence of such risk shall be documented and sufficiently reasoned, and the maximum period of one (1) month provided for may be extended for a period not exceeding three (3) months.

The person affected shall have the right to be heard at any time.

Likewise, the information concerning the person affected shall be treated with strict confidentiality.

5. Modification of the Internal Information System Policy

The Internal Information System Policy shall be reviewed periodically, and the management body shall be responsible for its approval and modification.

6. Approval and entry into force

The Internal Information System Policy shall become effective on the following day after its approval.