Internal Information System and Whistleblower Protection Policy

February 2026

1. INTRODUCTION TO THE INTERNAL INFORMATION SYSTEM

Grupo GIRÓ's position of leadership and excellence is the culmination of many years of effort and work. However, inappropriate behaviour from just one of its employees is enough to damage its image and reputation. Therefore, Grupo GIRÓ wants to actively prevent and avoid this possibility by establishing a strong culture of compliance within the organisation, driven by the Board of Directors[1] and Senior Management.

As such, among other things, all employees and collaborators acting on behalf of and/or for Grupo GIRÓ are required to act in accordance with, respecting at all times: (i) current legislation, (ii) the Code of Ethics and (iii) internal policies, rules and procedures. In these prevention efforts, the cooperation of all employees is also of great importance when it comes to detecting possible irregular conduct.

In this regard, current legislation (*and especially the current Penal Code, after its reform in 2010 and 2015, and Circular 1/2016 of 22 January from the State Attorney General's Office*) reinforces the need for companies to have '**models for the prevention of criminal risks**'; in other words, control systems and mechanisms that allow them to prevent, detect and react to the risk of any of their members committing a crime for their benefit. According to article 31bis.5.4 of the Penal Code, one of the basic requirements that these models must meet is the obligation to inform the body in charge of monitoring the operation and observance of the prevention model of possible risks and non-compliance, so a mechanism that allows for the reporting of said risks and non-compliance must be established in the company. In the case of Grupo GIRÓ, this mechanism is embodied in the Internal Information System.

With the publication of the Whistleblowing Directive 2019/1937 and its recent transposition into all European Union member states, protection measures for whistleblowers of sanctions or infringements within the company were expanded.

Specifically, the aforementioned Directive was transposed in Spain by Law 2/2023 of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter Law 2/2023), which came into force on 2 July 2023; in Germany through the HinSchG (Hinweisgeberschutzgesetz) or German Whistleblower Protection Act, and in Italy through Legislative Decree of 10 March 2023, No. 24.

As for the United States, there are no identified rules that set out specific criteria for the Internal Information System of the subsidiary Giro Pack, Inc. Nevertheless, the guidelines issued by the Department of Justice to date can serve as a reference for good practices to be taken into account.

In **Mexico**, currently there is also no **comprehensive law on whistleblowing**. Instead, the protection of those who report irregularities relies on various legal regulations and mechanisms **in a more**

[1] The Board of Directors is understood to be that of the Group's parent company, GIRNET INTERNACIONAL, S.L, without prejudice to the fact that the Internal Information System is made available to the Group by the entity GIRO GH, S.L.

fragmented or indirect way, especially in the context of combating corruption and administrative responsibilities. Part of the protection is found within the General Law of Administrative Responsibilities and the National Anti-Corruption System, with obligations for reporting mechanisms and, in some cases, protection of the whistleblower.

Grupo GIRÓ scrupulously complies with all legal requirements regarding privacy and data protection in the management of the Internal Information System. The System's management is supervised by the Internal Information System Manager. Their main function is to ensure that information is received, processed, and resolved appropriately and effectively. This person has a duty of confidentiality and will ensure that, for any complaint made (from the receipt of the information to its investigation), the identity of the person making the complaint is duly preserved and treated with the utmost confidentiality, if so desired.

Grupo GIRÓ wishes to highlight that any individual may report both through the Internal Information System whose compliance policy is regulated by this document, and through external information bodies, whether they are whistleblower protection authorities of each state, or autonomous or regional bodies, or the European Union.

For Spain, the competent external information body would be the Independent Authority for the Protection of Whistleblowers (https://www.proteccioninformante.gob.es/procedimiento-de-solicitud-de-proteccion), the autonomous authorities or bodies, or the European Union.

As for subsidiaries, if the information affects the German subsidiary GIRO GmbH, it can be reported through the Federal Office for External Complaints of the Federal Office of Justice (https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Hinweisgeberstelle/hinweisgeberstelle_node.html); the External Complaints Office of the Federal Competition Service (https://www.bundeskartellamt.de/DE/Kartellverbot/Hinweisgeberschutz/hinweisgeberschutz_node.html) and the Complaints Centre of the Federal Financial Supervisory Authority (https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html).

If the information affects the Italian subsidiary GIRO ITALIA S.R.L. You can report through the National Anti-Corruption Authority (ANAC), which is the national external authority designated in Italy to receive and manage external reports of complaints (segnalazioni), that is, complaints that are not submitted through the internal channel of the organisation itself.

In the United States, information can be reported through the official website of the United States Department of Labor: https://www.dol.gov/

In Mexico, there is currently no single, specific national authority equivalent to the European whistleblower protection authorities, nor a generalised system of external whistleblowing channels for the private sector. However, individuals wishing to report irregularities or potential illegal acts may, depending on the nature of the facts, contact the competent public authorities, in particular: The authorities comprising the National Anti-Corruption System, through the citizen complaint platforms enabled for this purpose, and the competent administrative, tax, labour or criminal authorities according

to the subject matter of the communication (for example, anti-corruption authorities, tax authorities or judicial authorities).

Grupo GIRÓ guarantees confidentiality when the communication is sent by whistleblowing channels other than those established or to members of staff not responsible for its processing, who will have been trained in this matter and warned that any breach is classified as a very serious infringement and, likewise, of the establishment of the obligation of the recipient of the communication to send it immediately to the System Manager.

All references in this document and its annexes to data protection shall be understood to be made in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation or GDPR), in accordance with the transposition legislation in force in each country, which in Spain has been transposed through the Organic Law 3/2018 (LOPD), in Germany through the Bundesdatenschutzgesetz (BDSG) of 30 June 2017, and in Italy through Legislative Decree No. 196 of 30 June 2003, Code on the protection of personal data, amended and adapted by Legislative Decree No. 101 of 10 August 2018.

2. WHO CAN REPORT THROUGH THE INTERNAL INFORMATION SYSTEM?

The Internal Information System (or "IIS") is aimed at all professionals in the companies that make up Grupo GIRÓ in Spain: GIRNET INTERNACIONAL, S.L., GIRO GH, S.A., GIRO INVEST XXI, S.L., NOVOTECNO, S.A., and SERFRUIT, S.L. (for the purposes of this document, we will refer to all of them as '**Grupo GIRÓ**' or the '**Group**' indistinctly), i.e., it can be used by all employees, workers' representatives, managers, shareholders, participants and members of the administrative, management or supervisory body (hereinafter, jointly and indistinctly, '**Members of Grupo Giró**').

For the purposes of this document, an employee shall be understood to mean any natural person who, by virtue of an employment relationship and under the organisation and direction of any of the companies that make up Grupo GIRÓ, provides their services on a regular basis for a fee, including both those with an employment contract, as well as students, volunteers, interns and trainees.

The IIS can also be used by those whose employment relationship has not yet begun, in cases where information on infringements has been obtained during the selection process or pre-contractual negotiation.

It can also be used by any of Grupo Giró's clients, external collaborators, agents, distributors or suppliers, or natural persons who work for or under their supervision and direction who wish to make Giró aware of risks or breaches that affect Grupo Giró, by natural or legal persons providing support to persons who provide information through the IIS or who are related to the informant, and legal entities for whom they work or with whom they maintain any other type of relationship in an employment context or in which they hold a significant stake.

All persons mentioned have the right to have the confidentiality of their information respected.

3. WHO MAY BE AFFECTED BY THE INFORMATION PROVIDED THROUGH THE INTERNAL INFORMATION SYSTEM?

Any member of Grupo Giró and any third party who, based on a commercial or collaborative relationship, represents, acts or provides services on behalf of or for Grupo Giró may be affected.

During the processing of the file, the persons affected by the communication will have the right to the presumption of innocence, the right to defence and the right of access to the file under the terms established by the legislation transposing the provisions of the Directive, where applicable, as well as the same protection established for the informants, preserving their identity and guaranteeing the confidentiality and data of the procedure.

4. WHAT MUST BE REPORTED?

In accordance with the legislation that transposes the provisions of the Directive, through the System any actions or omissions that may constitute infringements of European Union law, or, where applicable, the law applicable to the state where the subsidiary affected by the infringement is located, may be reported, as well as actions or omissions that may constitute a serious or very serious criminal or administrative offence, also encompassing possible risks or breaches or conduct contrary to the Group's Code of Ethics or any internal and/or external regulations with criminal or non-criminal implications.

The Internal Information System may not be used to communicate personal matters or matters that fall outside the scope of the objective defined in the preceding paragraphs.

It should also be noted that, in Spain, according to the provisions of Article 456 et seq. of the Penal Code, false accusation, false reporting and the simulation of crimes are considered crimes, punishable by imprisonment for up to two years.

On the other hand, as indicated in the Grupo Giró Code of Ethics, any doubts regarding legal or ethical breaches with or without criminal implications, or the formulation of a complaint or suggestion regarding the operation of the Grupo Giró Compliance and Criminal Prevention Model, can also be made by contacting the Grupo Giró Criminal Risk Prevention Officer directly through the channels provided for the Internal Information System indicated in the following section.

5. HOW SHOULD INFORMATION BE PROVIDED?

5.1 Procedure

The Internal Information System can be accessed in the following ways:

- By email: **crp@giropack.com**.
- By phone: +34 659 78 16 47

- Postal address: c/ Jaume Ribó 35-37 1º Badalona 08911, to the attention of the Criminal Risk Prevention Officer.

At the informant's request, a face-to-face meeting may also be requested through the above channels within a maximum period of 7 days.

When offering information, it is recommended to provide:

- An address or means for notification to be informed of any updates regarding the communication (email, postal mail, telephone).
- The name and surname of the affected person(s).
- The Department/Area to which the affected person(s) belong.
- A description of the events.
- Evidence or supporting documentation on which the information is based, if available.

The person providing the information is not compelled to provide their identity but it is advisable in order to facilitate the investigation.

For informational purposes, the identity of those with the main roles within the Internal Information System are as follows:

Internal Information System Manager: Abel Perpiñán Hinarejos

Criminal Risk Prevention Officer: María Pilar Miñana Moliner

Head of the Human Capital Department: Erick Barckhahn Delpiano

If the information is provided by telephone or through a voice messaging system, or through verbal communication in a face-to-face meeting, the informant will be advised that the communication will be recorded and will be informed of the processing of their data in accordance with the provisions of EU Regulation 2016/679 of 27 April 2016.

All verbal communications, including those made in face-to-face meetings, by telephone or through voice messaging systems, must be documented by means of a recording of the conversation in a secure format or through a complete and accurate transcript of the conversation made by the staff responsible for handling it. The informant has the right to review the transcript before considering it final.

Once the communication has been provided, the informant will be sent an acknowledgment of receipt of the communication made, within a maximum period of 7 calendar days, unless this could jeopardise the confidentiality of the communication.

The more information that can be provided about the reported events, the easier and faster the investigation will be.

5.2 Can information be provided anonymously?

Informants can opt to identify themselves when providing information, but information provided anonymously will also be accepted. However, informants are encouraged to identify themselves in order to obtain more information about the reported events. Maximum confidentiality will be assured regarding the identity of any informant who wishes to be identified.

Initially, the informant's identity will only be known to the Information System Manager and the Criminal Risk Prevention Officer. Other people within Grupo Giró will not have access to these details unless it is necessary to obtain more information about the facts.

All persons who, through the functions they perform in Grupo GIRÓ, become aware of the communications that are made are obliged to maintain professional secrecy regarding the identity of the informant.

It is expressly stated that the exercise of the right of access by the persons to whom the reported facts refer, which is recognised by the regulations on the protection of personal data, does not imply access to data relating to the identity of the informant. Therefore, and as a general rule, the person being investigated or affected by the communication will not know the identity of the informant.

However, exceptionally and provided there is a justified cause of sufficient importance, the processing of data by other persons, or even its communication to third parties, will be lawful when it is necessary for the adoption of corrective measures in the entity or the processing of the sanctioning or criminal procedures that may be appropriate. For example, it might be necessary to disclose the informant's identity to relevant parties outside the organisation who are involved in the investigation or legal proceedings that may be initiated as a result of a detected violation. In such cases, before revealing their identity, the informant will first be informed of this circumstance.

Information on the processing of personal data within the framework of the Internal Information System can be found in the Privacy Policy of the Internal Information System included in Annex I to this document.

6. WHAT ARE THE CONSEQUENCES FOR THE INFORMANT OF PROVIDING INFORMATION?

Any person who provides information, whether through the Internal Information System or through public disclosure, who has reason to believe that the information is truthful, and who has done so in accordance with the provisions herein and in good faith, is protected against any type of retaliation, discrimination or penalty on account of the same. The Group will ensure protection measures against retaliation and provide other support measures.

The prohibition of retaliation provided for in the preceding paragraph shall not prevent the adoption of appropriate disciplinary measures when the internal investigation determines that the communication is false and that the person who made it was aware of its lack of veracity, having acted in bad faith.

****

Annex I

INTERNAL INFORMATION SYSTEM PRIVACY POLICY

1. PURPOSE

The purpose of this Privacy Policy of the Grupo GIRÓ Internal Information System is to provide information about the processing of data that will be carried out for the management and processing of communications submitted through it.

2. DATA CONTROLLER

The data controller is GIRÓ GH, S.A., with address at C/ Jaume Ribó 35-37, 1° B 08911 Badalona (Barcelona).

The Internal Information System managed by GIRÓ GH, S.A. serves and is accessible to all companies in the Giró Group in Spain, therefore GIRÓ GH, S.A. has signed data processing agreements with all of them, namely: GIRNET INTERNACIONAL, S.L., GIRO INVEST XXI, S.L., NOVOTECNO, S.A., and SERFRUIT, S.L., which include all the provisions required by Article 28 of the aforementioned Regulation 2016/679.

3. SOURCE OF PERSONAL DATA

The Internal Information System will process the personal information of the informant and the affected party, as well as third parties involved in the events being reported or related to inquiries made.

This information may be provided: (a) by the informant or interested party (b) by any of the other persons involved in the investigation, with respect to the remaining persons, or (c) by any of the companies of the Giró Group, by virtue of their status as employer of the same.

4. LAWFULNESS, PURPOSE AND LEGAL BASIS

In accordance with the legislation that transposes the provisions of the Directive, and always in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the processing of personal data that is necessary for the application of said law, as well as the processing of personal data from internal communications, external communication channels, those derived from a public disclosure and those of special categories of personal data for reasons of an essential public interest, are considered lawful.

Personal data collected in the Internal Information System will be processed for the sole purpose of handling incoming communications and, where appropriate, investigating the veracity of reported facts or conduct, always preserving the identity of the informant and ensuring adequate protection against reprisals that reporting individuals may suffer, strengthening the culture of information, the integrity infrastructures of organisations, and promoting a culture of information or communication as a mechanism to prevent and detect threats to the public interest.

Finally, in some cases personal data may also be processed to comply with certain legal obligations applicable to the company. In these cases, and to the extent possible, information will be provided about this and the rule that imposes it.

5. DATA RETENTION PERIOD

The data of the person providing the information, the affected party, Members of Grupo Giró and third parties (Suppliers, Associates, etc.) who participate in the investigation of information will be kept in the internal information system initially for the time necessary to (a) decide on the appropriateness of initiating an investigation into the reported facts and, if applicable, (b) for the time during which the relevant investigation is carried out (within the organisation).

If the information received contains personal data included within the special categories of data, it will be immediately deleted, without being recorded and processed.

The processed data will only be kept for the time necessary to decide on the appropriateness of initiating an investigation into the reported facts.

If it is proven that the information provided or part of it is not truthful, it will be immediately deleted from the moment that such circumstance is known, unless such lack of truthfulness may constitute a criminal offence, in which case the information will be kept for the time necessary for the judicial procedure to be processed.

In any case, if three months have passed since the receipt of the communication and no investigation has been initiated, it will be deleted, unless the purpose of its preservation is to provide evidence of the functioning of the system.

Communications that have not been processed may only be recorded anonymously, without the data retention obligation being applicable.

Employees and third parties must be informed about the processing of personal data within the framework of the Information Systems.

In no case may data be stored for a period exceeding ten (10) years.

6. LIMITATION ON ACCESS TO DATA. WHO WILL YOUR DATA BE TRANSFERRED TO?

Access to personal data contained in the Internal Information System will be limited, within the scope of their powers and functions, exclusively to:

a) The Information System Manager and the Criminal Risk Prevention Officer.

b) The Head of the Human Capital Department or the duly designated competent body, only when the adoption of disciplinary measures against a worker may be appropriate.

c) The Head of Legal Services of the entity or body, if different from the Criminal Risk Prevention Officer and if the adoption of legal measures is appropriate in relation to the events reported in the communication.

d) The data processors who may be appointed.

e) The Data Protection Officer.

The processing of data by other persons, or even its communication to third parties, will be lawful when it is necessary for the adoption of corrective measures in the entity or the processing of the sanctioning or criminal procedures that may be appropriate.

Personal data that is not necessary for the knowledge and investigation of the reported actions or omissions will never be processed, and where appropriate, it will be immediately deleted. Likewise, all personal data that may have been communicated and that refers to conduct not included in the scope of application of the law will be deleted. If necessary for the adoption of corrective measures in the entity or the processing of the corresponding sanctioning or criminal proceedings, the data may be communicated to those third parties to whom it is legally obliged to provide them, such as Public Bodies, Judges and Courts or Law Enforcement Agencies.

Likewise, Grupo GIRÓ collaborates with third-party service providers who may have access to your personal data and who will process said data on its behalf.

In relation to the above, it should be made clear that Grupo GIRÓ follows strict criteria for selecting service providers in order to comply with its data protection obligations and undertakes to sign the corresponding data processing contract with them, through which it will impose, among others, the following obligations: to use appropriate technical and organisational methods; to process the data only for the agreed purposes and only according to the documented instructions of Grupo GIRÓ and to delete or return the data once the provision of services is completed.

Specifically, Grupo GIRÓ may engage the services of third-party providers that carry out their activity, including but not limited to, in the following sectors: legal advice, multidisciplinary professional services companies, or companies that provide technological or IT services.

7. EXERCISING RIGHTS

a) Individuals whose personal data may be processed within the framework and context of the Internal Information System have the right to receive the information contained in this annex, in compliance with the provisions of Article 13 of the GDPR. Thus, they will have the right to obtain confirmation as to whether or not their personal data is being processed by Grupo GIRÓ (within the framework of the management of the Internal Information System), as well as to access, rectify, limit the use of their data, or, where appropriate, request its erasure, under the legally established terms, when, among other reasons, the data is no longer necessary for the management of the Internal Information System.

b) In certain circumstances, to oppose the processing of their personal data.

Grupo Giró has appointed a Data Protection Officer to ensure that it complies with all legal requirements of the regulations on the protection of personal data, both at a national and European level. This person will be responsible for providing all the necessary information regarding the processing of personal data.

The Data Protection Officer can be contacted via rgpd@giro.es, and both informants and those affected by the information may address any question relating strictly to the processing of their personal data, as well as for the exercise of their legitimate rights in matters of privacy.

Complaints may also be lodged with the Spanish Data Protection Agency (as the competent supervisory authority in matters of data protection), especially when no satisfactory resolution has been obtained in exercising rights through the Data Protection Officer, by writing to the Spanish Data Protection Agency at C/ Jorge Juan, 6 28001-Madrid or via the website https://www.aepd.es.

In the case of subsidiaries, information can be provided through the competent external reporting body in accordance with each regulation.

8. PRINCIPLE OF PROPORTIONALITY AND DATA MINIMISATION

- ✓ Personal data collected within the framework of the Internal Information System: will be limited to what is strictly and objectively necessary to process the inquiries, the information and, if appropriate, to verify the reality of the reported facts;
- ✓ will be processed at all times in accordance with applicable data protection regulations, for legitimate and specific purposes in relation to any investigation that may arise as a result of the communication.
- ✓ will be adequate and not excessive in relation to the aforementioned purposes.

9. SECURITY AND CONFIDENTIALITY MEASURES

Grupo GIRÓ will ensure that all necessary technical and organisational measures are taken to preserve the security of the data collected, whether relating to the informant(s) or the person(s) subject to the information, in order to protect them from unauthorised disclosures or access.

To this end, Grupo GIRÓ has adopted appropriate measures to guarantee the confidentiality of all data and will ensure that data relating to the identity of the informant are not disclosed to the affected party during the investigation, except with the express written consent of the informant, respecting in all cases the fundamental rights of the person, without prejudice to the actions that may be taken by the competent judicial or administrative authorities, where applicable.

These security and confidentiality measures will only be waived if so ordered by the competent judicial or administrative authority, or when both the informant(s) and the subject(s) of the information so allow in writing.

Informants will be entitled to the protection and support measures provided by the legislation transposing the provisions of the Directive. Acts constituting retaliation, such as suspension of the employment contract, dismissal, or termination of the employment relationship, damages, including reputational damages, or economic losses, coercion, intimidation, harassment or ostracism, negative evaluation or references, inclusion on blacklists, denial or cancellation of a licence or permit, denial of training and discrimination, are expressly prohibited.