

Internal Information System Policy



Date	Review	Responsible	Subject	Significant changes
	0	Compliance Committee	New wording	

CONTENTS

Target.....03

Scope..... 04

Applicable regulations.....04

Definitions.....05

Internal Information System. 06

Principles..... 09

Guarantees..... 11

External channel..... 12

Upgrade and Upgrade..... 13

Training..... 13

Compliance Committee..... 13

Formulation of concerns and reporting of non-compliance.....13

Dissemination and publicity of politics.....14

Approval.....14

Annex I.....15

1. OBJECTIVE

On 13 March, Law 2/2023, of 20 February, regulating the protection of people who report regulatory breaches and the fight against corruption, came into force.

The ultimate purpose of this regulation is to guarantee the protection of those citizens who, in a work or professional context, report possible violations of the legal system within the framework of said relationship.

With this, and with the aim of complying with this regulation, this policy contains a description of the key elements, both human and organisational, technological and documentary, that Freixenet Iberia ¹ will apply to protect the information received by the Informants, as well as the personal data.

It will also include the creation of an Internal Information System (hereinafter, "S.I.I."), and will enunciate the general principles in terms of the defense of the Informant, describing its operation, the internal channel enabled, the times to be fulfilled, and the Person Responsible for said system.

Thus, as a company we want to inform all people who have a professional or employment relationship, of the possibility of reporting irregular practices that take place in the organization itself through the mechanism established in this policy and that will be detailed later, in order to correct it or repair possible damages as soon as possible.

The organisation makes a single internal channel available to anyone who has an employment or professional relationship, guaranteeing confidentiality in all cases, as well as giving them the possibility of informing anonymously, if they prefer.

At all levels of Freixenet Iberia, the real and effective application of this Policy will be ensured in such a way as to adequately protect Whistleblowers from possible reprisals they may suffer, as well as to strengthen the information culture in the company.

Freixenet Iberia will apply a zero-tolerance criterion with respect to any act of retaliation that a Whistleblower may suffer when he or she transmits or makes known through the internal channel provided for in this Policy any act or omission that may constitute an infringement of European Union Law or a serious or very serious criminal or administrative infringement for the purposes provided for in the regulation in question.

All members of Freixenet Iberia should thoroughly familiarize themselves with this policy, as well as with other policies and procedures and the Code of Conduct of the Geschwister Oetker Group.

This policy is part of a broader compliance programme and other policies and procedures may include more specific areas on legal and compliance risks or other requirements depending on

¹ Freixenet, S.A.; Segura Viudas, S.A.U., Comercial Grupo Freixenet, S.A.; and Unió Cellers del Noya, S.A. as well as any other Spanish subsidiary or majority-owned company in which Freixenet, S.A. is directly or indirectly effectively controlled.

each country. Members of Freixenet Iberia should refer to these other policies and procedures to have greater knowledge about specific situations and, if they have any questions or require any clarification, they should contact their hierarchical superior (if applicable) or the Compliance Committee.

This policy will be adapted to the normative and regulatory changes that occur in the future.

2. SCOPE OF APPLICATION

- a. **Corporate scope:** This policy applies to all the companies that make up Freixenet Iberia, as well as to Third Parties as indicated below.
- b. **Personal scope:** This policy is applicable to all levels of Freixenet Iberia, including administrative bodies, management positions, control bodies, all staff. Persons who have the status of employees of Freixenet, and self-employed persons, shareholders and persons belonging to the administrative, management or supervisory body of Freixenet, including non-executive members. Any person who works under the supervision and direction of contractors, subcontractors and suppliers of Freixenet. Also included are whistleblowers who communicate or publicly disclose information on infringements obtained within the framework of an employment or statutory relationship that has already ended, voluntary staff, interns, trainees regardless of whether or not they receive remuneration, as well as those whose relationship has not yet begun, in cases where the information on the infringement has been obtained during the selection process or pre-contractual negotiation.
- c. **Relational scope:** the scope of application of this policy will extend to the Freixenet Iberia 's suppliers, distributors and customers.
- d. **Geographical scope:** This policy will be applied at the national level, thus complying with the Spanish and European legislation that may apply.

3. APPLICABLE REGULATIONS

This policy is drafted to comply with the following regulations:

- a. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.
- b. Law 2/2023, of 20 February, regulating the protection of people who report regulatory breaches and the fight against corruption.
- c. Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.

4. DEFINITIONS

a). Informant

The term "Informant" means:

- Any person who reports violations of the legal system within the framework of a professional or employment relationship.
- Any person who reports breaches of the legal system, even if their professional relationship has ended, volunteers, trainees or trainees, people who participate in selection processes, as well as people who provide assistance to informants, people around them who may suffer reprisals, as well as legal persons owned by the informant, among others.

b). Violation of the legal system

It will be considered as violations of the legal system and, therefore, will be issues that can be reported through the internal channel enabled:

- Actions or omissions that may constitute infringements of European Union law².
- Actions or omissions that may constitute serious or very serious criminal or administrative offences as provided for in the aforementioned regulations.

c). Third parties

The term "Third Parties" means any supplier, distributor, consultant, agent, broker or other natural or legal person who is not part of Freixenet Iberia and who has a professional relationship with the organisation.

d). Retaliation

Any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the people who suffer them at a particular disadvantage with respect to others in the work or professional context, solely because of their status as Informants, or because they have made a public disclosure.

5. INTERNAL INFORMATION SYSTEM

As briefly explained in the introduction, the existence of an Internal Information System in the company is hereby confirmed, which will allow, through a single internal channel enabled, to

² The following sectors are included: public procurement, services, financial products and markets, and prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental and climate protection, radiation protection and nuclear safety, food and feed safety, animal health and animal welfare, public health, consumer protection, protection of privacy and personal data, and security of networks and information systems.

communicate any type of infringement of those mentioned above, guaranteeing the confidentiality of the Informant and any other person mentioned in said communication, preventing in any case the access of unauthorized personnel.

The Administrative Body is responsible for the implementation of the S.I.I. and will have the status of Controller of Personal Data in accordance with data protection regulations.

Thus, it is worth mentioning that, given that the integrated platform is structured within the Henkell Freixenet group's system, Mr. José Luis Abel Lluch, current Compliance Coordinator of the Henkell Freixenet group, will act as external manager of the Internal Information System, not being able to classify or filter the information, but simply receive and read it. In this case, Mr. Herrmann will act as data protection officer for the purposes of the legislation on personal data protection, guaranteeing at all times the guarantees of respect for independence, confidentiality and data protection.

To do this, the company will:

- A. It has integrated all the existing channels into a single internal channel that allows communications to be presented both verbally, directly addressed to the Information System Manager, and in writing through the platform specified below.
- B. Has appointed a Head of the SIS.
- C. It has an information management procedure that effectively treats the communications received.

5.1. Internal information channel integration

Until now, the organization had different internal communication channels, depending on the specific subject matter.

1. Firstly, under the Anti-Harassment Protocol, the complaint or request for support and assistance was made to the reference persons listed in the annex attached to it, both verbally and in writing and through any means.
2. Secondly, in terms of data protection, anyone could contact the Data Protection Officer (DPO) directly via the following email address gdpr@freixenet.com.
3. Thirdly and finally, anyone could report such allegedly irregular generic conduct, through one of the following channels:
 - a. Immediately go to the Compliance Committee;
 - b. Contact the organisation through the Freixenet Iberia's Communication System:

- Sending anonymous messages: www.report-securely.eu/henkell-freixenet;
- Sending non-anonymous messages by email to the Compliance organisation of Freixenet Iberia Spain: compliance@freixenet.com;
- Sending non-anonymous messages by e-mail to the Compliance organization of the Henkell-Freixenet International Group: compliance@henkell-freixenet.com.

With the entry into force of this regulation, the previous existing channels will be integrated into **a single channel**. This internal information channel can be accessed, which allows written communications (and anonymously if preferred) to be made through the following platform: www.report-securely.eu/freixenet

This single channel allows communications between the Informants and the System Manager, even if they are anonymous, in order to be able to collect all the information that may be necessary to initiate the investigation, and additional information may be requested from the Informant, if deemed necessary.

Notwithstanding the foregoing, at the request of the Informant, a face-to-face meeting may be requested. In this case, the Informant will be warned that the communication will be recorded and will be informed of the processing of their data in accordance with the provisions of current data protection regulations.

5.2. Responsible for the Internal Information System

The board of directors has appointed Mr. José Luis Abel Lluch, current Chief Financial Officer and member of the Freixenet Iberia 's Compliance Committee, as the Head of the Internal Information System, who will be responsible for managing this system. In the event that Mr. Abel is away from the office, Mr. Josep Palau, current Chief Technology Officer and member of the Compliance Committee, will become the Head of the Internal System.

Without prejudice to the foregoing, and depending on the specific subject matter of the communication received, Mr. Abel, and in his absence Mr. Palau, will initiate the pertinent investigations with the manager that is necessary in each case, always guaranteeing the confidentiality of the Informants and Third Parties that appear in the communications, as well as their content.

The structure of the Internal Information System is detailed in **Annex I** attached to this policy.

5.3. Information management procedure

This information management procedure pursues the objective of clarifying the way in which any Informant can report any act or omission and be aware of the deadlines and guarantees that will be available:

- a) As specified in section 5.1., there is currently only a single internal channel, which can be accessed through the following hyperlink: www.report-securely.eu/freixenet On this platform there will be two options:
 - 1. Firstly, the option to send a new communication, either anonymously or with confidentiality of identity, both manifestly, and,
 - 2. Secondly, the possibility of following up on a communication that has been made anonymously.
- b) When making the communication, and in the event that he/she wishes to remove his/her anonymity, the Informant may indicate his/her name and an email address for the purpose of receiving notifications.
- c) Likewise, the platform will ask you to create a secure password in order to access the mailbox of the information sent, check the processing status, as well as communicate with the Information System Manager.
- d) Whether the communication is anonymous or not, the Informant may follow up on the status of their communication with the reference ID and the individual password assigned at the time they submitted their communication. Likewise, if they have provided an email address, the Informant will receive the reference ID at that address, as well as the acknowledgement of receipt of the communication sent within a maximum period of seven (7) calendar days, unless this may jeopardize the confidentiality of the communication.
- e) In the event that a face-to-face meeting is requested, it will be held within a maximum period of seven (7) days.
- f) The person concerned shall have the right to be informed of the actions or omissions attributed to him, and to be heard at any time. Such communication shall take place at the time and in the manner deemed appropriate to ensure the successful completion of the investigation.
- g) The System Manager, together with the managers specified according to the matter in question, will respond to the investigation actions within a maximum period of three (3)

months from the receipt of the communication, except in cases of special complexity that require an extension of the period, in which case, it may be extended to a maximum of another three (3) additional months.

- h) The information will be sent to the Public Prosecutor's Office immediately when the facts could constitute an offence. In the event that the facts affect the financial interests of the European Union, it will be sent to the European Public Prosecutor's Office.

6. PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

The company's strategy for the protection of persons who report regulatory violations will comply with the principles of confidentiality, integrity, authenticity and traceability of information, presumption of innocence and protection of personal data:

- a) Confidentiality

The principle of confidentiality ensures that information is only accessible to users authorised to access it and that it may not be disclosed to third parties without the corresponding authorisation.

Thus, extreme confidentiality is ensured at all times in the Information received, as only the System Manager, as well as the managers designated according to the matter, will have access to the communications received in question.

Likewise, this confidentiality is guaranteed even when the Information is sent through a whistleblowing channel other than the one established and delimited in this policy. Therefore, staff will be trained so that they are aware of the obligation to transfer any Information of this nature to the System Manager, as well as of the infringement of breaching said confidentiality.

- b) Integrity

The principle of integrity ensures that information is kept free of modification and that it has not been altered by people or processes.

- c) Authenticity and traceability of information

The principle of authenticity and traceability of information guarantees that the relevant investigations will be carried out as a result of the information received to ensure the authenticity of the acts and, if so, to apply the measures that repair or avoid possible damage as much as possible.

d) Presumption of innocence

All persons affected by communications will have their innocence and honor until it is reliably demonstrated through the investigations carried out, to the contrary.

e) Protection of personal data

All personal data processed under the Internal Information System and its communications will comply with current data protection regulations.

The data will be kept in the information system only for the time that is essential to decide on the admissibility of initiating an investigation into the facts reported.

If it is proven that the information provided or part of it is not true, it will be immediately deleted from the moment that this circumstance is known, unless such lack of veracity may constitute a criminal offence, in which case the information will be kept for the necessary time during which the judicial proceedings are being conducted.

In any case, if three (3) months have elapsed since receipt of the communication without any investigation proceedings having been initiated, it will be deleted, unless the purpose of the conservation is to leave evidence of the operation of the system.

The company will destroy information that does not need to be stored or that has exceeded the period established for its retention. Likewise, the company will also have a blocking procedure, which will prevent access to the information by any unauthorized person, as well as the processing of blocked personal data.

In view of the data to which the company will have access by virtue of such communications, it will inform the Informant of its duty to know and will comply with the regulations on the protection of personal data contained in the Law, and especially the obligation not to disclose, disseminate or make use to third parties of information that may be considered of a personal nature to which it has access.

7. GUARANTEES OF THE INTERNAL INFORMATION SYSTEM (SII)

7.1. Protection conditions

The Internal Information System, as well as the Information Management Procedure received through the single internal channel enabled, will have a series of guarantees, with the aim of facilitating such communications and defending the Informant at all times.

Persons who report or disclose offences as defined in paragraph 4(a) shall be entitled to protection provided that the following circumstances are met:

- a) There are reasonable grounds for the veracity of the possible infringement;
- b) The communication has been made in accordance with the requirements set forth in this policy, as well as in the regulations in force;
- c) It has been made in good faith and,
- d) It is within the scope of protection of the Law.

Persons who communicate or reveal:

- a) Information contained in communications that have been inadmissible by the internal information channel because they are:
 - a. Facts reported that lack any verisimilitude.
 - b. Facts reported that do not constitute an infringement of the legal system.
 - c. Communication without foundation or obtained through the commission of a crime.
 - d. Reporting without new and meaningful information on infringements compared to a previous communication for which the relevant procedures have been concluded, unless there are new circumstances that warrant a different follow-up.
- b) Information related to complaints about interpersonal conflicts or that affect only the Informant and the persons to whom the communication or disclosure refers.
- c) Information that is already fully available to the public or that constitutes mere rumors.
- d) Information that refers to actions or omissions not included in the material scope of application of the regulations in force.

Persons who have publicly communicated or disclosed information about actions or omissions within the scope of the law in question but who have subsequently been identified and meet the conditions provided for in this law, shall be entitled to the same protection.

7.2. Prohibition of retaliation

In compliance with current regulations, Informants who communicate through the channel enabled in the Internal Information System will not be exposed to any reprisals.

The Whistleblower shall be protected from retaliatory measures for a period of two (2) years.

8. EXTERNAL INFORMATION CHANNELS

In addition to the internal channel within the organisation, it is important to highlight the existence of external channels of information before the competent authorities and, where appropriate, before the institutions, bodies or agencies of the European Union.

Specifically, any natural person may report to the Independent Authority for the Protection of Whistleblowers (A.A.I.) or to the corresponding authorities or regional bodies, the commission of any actions or omissions, either directly or after communication through the detailed internal channel.

The information to the A.A.I. may be made in writing, through postal mail or through any electronic means enabled for this purpose addressed to the external information channel of the A.A.I., or verbally, by telephone or through a voice messaging system. At the request of the Informant, it may also be presented through a face-to-face meeting, within a period of seven (7) days.

On the date of approval of this policy and in the territorial scope of Catalonia, the body that will perform the function of A.A.I. is the Anti-Corruption Office of Catalonia.

9. UPDATING AND IMPROVING THIS POLICY

The company will carry out a constant verification of the application of this standard and will propose the appropriate modifications in the following circumstances:

1. When legal changes occur.
2. When there are changes in the guidelines and criteria of the control authorities.

10. TRAINING

Those members of Freixenet Iberia who are involved and who are part of the Internal Information System will receive training on the procedure to be followed in the event of receipt of information in order to comply with the requirements required by law, i.e. response deadlines, guarantee of confidentiality, non-retaliation, etc.

11. COMPLIANCE COMMITTEE

The Compliance Committee is an internal committee that has been established to supervise and evaluate the implementation and effectiveness of the Freixenet Iberia 's policies and procedures in terms of their compliance with applicable anti-corruption legislation.

12. FORMULATION OF CONCERNS AND REPORTING OF NON-COMPLIANCE

Freixenet Iberia wants to be promptly informed of any concerns that may arise regarding this policy, so that it can immediately address any possible problem. In the event of any doubt about this policy or any concern about a possible violation of it, the members of Freixenet Iberia should contact their hierarchical superior (if applicable), the Compliance Committee, the legal department or through the Communication System implemented in Freixenet Iberia as soon as possible.

Freixenet Iberia will not tolerate retaliation of any kind against those who have reported, in good faith, an alleged violation of the applicable laws, rules and regulations or of the internal policies and procedures of Freixenet Iberia.

13. DISSEMINATION AND PUBLICITY OF THE POLICY

This S.S.I. Policy will be published on the website and made available to all employees together with the Internal Information System Information Management Procedure included therein in section 5.3.

The Organization will disseminate this S.S.I. Policy and the Internal Information System Information Management Procedure, with the aim of making it known and promoting its use.

14. APPROVAL

The current Anti-Corruption Policy has been approved by the Board of Directors on 12 June 2023, and is mandatory for all employees of Freixenet Iberia.

ANNEX I: INTERNAL INFORMATION SYSTEM CONTROL STRUCTURE

The company, as already defined above, has a control structure aimed at facilitating the entry of communications and guaranteeing their confidentiality in all cases. It is based on the following work scheme:

Administrative Body	It represents the highest level of the Internal Information System, being responsible for its implementation after consulting the legal representation of the workers, as well as the person responsible for the processing of personal data in accordance with current data protection regulations. It is also responsible for appointing the person responsible for the management of said system.
Internal System Manager	Person responsible for the management of the Internal Information System. Will carry out his/her functions independently and autonomously with respect to the rest of the company's bodies. This position will be held by Mr. José Luis Abel Lluch, current Chief Financial Officer and member of the Compliance Committee. In his absence, Mr. Josep Palau, current Chief Technology Officer and member of the Compliance Committee, will hold this position.
Managers	Reference persons who, depending on the specific matter of the communication, will support the Head of the Internal System in carrying out the investigations that may be relevant: • Accounting, audits and internal financial controls (irregularities in accounting and auditing, financial misconduct within internal controls): Compliance Committee. • Corporate integrity (bribery, corruption and fraud, gifts and hospitality, document forgery, conflicts of interest, competition and antitrust, confidentiality and data protection breaches): Compliance Committee and Data Protection Officer where applicable. • Environment, health and safety (breaches of environmental and occupational health and safety

	regulations, including bodily injury and abuse): Compliance Committee, Head of the Environment Department and Coordinator of Occupational Risk Prevention when applicable. • Human Resources, Diversity and Respect in the Workplace (Discrimination, [Sexual] Harassment and Bullying, Human Rights Violations, Compensation, General Personnel Matters, Misconduct or Inappropriate Behaviour): Reference persons listed in the Annex to the Harassment Protocol in force, as well as Human Resources Manager where applicable. • Abuse/Misappropriation of Assets or Services (Unauthorized Use of Corporate Resources or Equipment for Non-Commercial Reasons, Theft of Corporate Property, Work Schedule Fraud): Compliance Committee and Human Resources Officer where applicable. • Other (other violations of rules, laws and guidelines, general suggestions for improvement and new ideas): Compliance Committee.
--	--