

The background of the lower half of the page is a photograph of a modern glass skyscraper. In the foreground, numerous white papers are shown in motion, as if being blown by a wind machine, creating a sense of dynamic activity. The papers are slightly blurred, emphasizing movement. The bottom of the page is overlaid with a solid blue gradient that contains the title text.

INTERNAL WHISTLEBLOWING PROCEDURE

CONTENTS

SCOPE.....	3
WHO CAN BECOME A WHISTLEBLOWER?	3
WHAT CAN A REPORT RELATE TO?	4
WHAT ABOUT CONFIDENTIALITY?	5
TO WHOM SHOULD THE REPORT BE MADE?.....	6
<i>Choosing the reporting procedure: internal or external</i>	6
<i>Internal reporting</i>	6
<i>External reporting</i>	6
<i>Public disclosure</i>	7
COLLECTION OF INTERNAL REPORTS.....	7
<i>Who to report to</i>	7
<i>Content of the report</i>	7
<i>Handling of the report</i>	8
<i>Receipt of the report</i>	8
<i>Analysis of the report</i>	8
<i>Investigation procedure for handling the report</i>	8
<i>Resolution – Follow-up on the report</i>	9
EXTERNAL REPORTING: REFERRAL TO AN AUTHORITY DESIGNATED BY LAW	9
DATA PROCESSING POLICY	10
<i>What data are processed?</i>	10
<i>Retention period</i>	10
<i>Data destruction and security measures</i>	11
<i>Personal data</i>	11
FOLLOW-UP ON REPORTS	12
PUBLICISING THE INTERNAL WHISTLEBLOWING PROCEDURE	12
KEY POINTS	12

SCOPE

The Whistleblowing Procedure is one of the pillars of the GINGER Group's Ethics & Compliance Policy.

This Procedure enables all GINGER Group employees and stakeholders to:

- report, in complete confidentiality and without fear of pressure or reprisals, information relating to a crime, offence, threat or harm to the public interest;
- report breaches or situations that contravene our Anti-corruption Code of Conduct or our Ethics Charter;
- obtain information on the progress of a report already made.

The French legal framework governing this procedure is as follows:

- the "Sapin II" Law¹ with regard to the provisions on the protection of whistleblowers (Art. 6-16) and the provisions on measures to fight corruption (Art. 17);
- the European Directive on the protection of whistleblowers²;
- French laws on the protection of whistleblowers and the collection and processing of reports made by whistleblowers³; and
- ordinary law regulations on the protection of individuals (in particular provisions concerning discrimination of all kinds, moral harassment, sexual harassment, etc.).

Where local regulations relating to whistleblowers in a country other than France are more protective and/or stringent, local legislation shall apply rather than this Procedure. Conversely, if this Procedure provides for more protective and/or stringent rules, this Procedure shall prevail.

WHO CAN BECOME A WHISTLEBLOWER?

Whistleblowers may be any internal or external stakeholder. In other words, they may be:

- GINGER Group **employees** (permanent employees, fixed-term employees, interns, apprentices and temporary workers);
- the Group's **corporate officers**;
- **third parties** who are in contact with the GINGER Group or who have interests in the GINGER Group, such as clients, suppliers, co-contractors, subcontractors, external experts, intermediaries, shareholders, the State, associations and trade unions.

¹ Law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and the modernisation of economic life, and its implementing decree No. 2017-564 of 19 April 2017. This Policy constitutes an 'internal procedure' within the meaning of the decree.

² Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of European Union law.

³ Organic Law No. 2022-400 and Ordinary Law No. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers and Decree No. 2022-1284 of 3 October 2022 on procedures for the collection and processing of reports made by whistleblowers

Furthermore, in order to qualify as a whistleblower, the law provides for the following cumulative conditions of eligibility:

- the whistleblower must be a **natural person**;
- the whistleblower must act **without direct financial gain**;
- the whistleblower must act in **good faith** (without intent to cause harm).

When the information has been obtained:

- the whistleblower who has no interaction with the Group must have personal knowledge of the information that he/she is reporting;
- the whistleblower who has interactions with the Group (employees, suppliers, etc.) may report information that he/she has personally obtained, as well as information that has been reported to him/her.

The whistleblower may choose to remain anonymous, which, from a practical point of view, may make it more difficult or even impossible to process the report or establish the truth of the facts.

WHAT CAN A REPORT RELATE TO?

Subject to the conditions of eligibility, a report that may constitute an alert consists of disclosing in good faith:

- a crime or offence:
 - for example: acts of corruption, influence peddling and money laundering;
- a breach or attempted concealment of a breach:
 - of the law or regulations
 - for example:
 - non-compliance with regulations on combating undeclared work, forced labour or child labour;
 - acts of moral or sexual harassment;
 - non-compliance with health and safety regulations at work;
 - non-compliance with environmental law;
 - European Union law;
 - an international commitment duly ratified or approved by France;
 - a unilateral act of an international organisation taken based on such a commitment;
- a threat or serious harm to the public interest;
- a breach of the GINGER Group's Ethics Charter;
- a breach of the GINGER Group's Anti-corruption Code of Conduct;
- a breach of Group procedures;
- acts of reprisal related to the act of making a report or of participating in its processing;
- disclosure of confidential information;
- data theft, fraudulent appropriation of assets;
- financial statement fraud;
- human rights violations.

Whistleblowers may not disclose information covered by National Defence confidentiality, medical confidentiality or the confidentiality of relations between lawyers and their clients.

Only information that is unlawful or harmful to the public interest may be reported or disclosed. Simple malfunctions within a public or private entity cannot constitute grounds for whistleblowing.

Only a person who meets the above criteria can be considered a whistleblower and thus benefit from the whistleblower protection regime provided for by law. This protection guarantees their anonymity.

Whistleblowers who act in good faith without direct financial gain cannot be excluded from recruitment procedures or access to internships or professional training.

When the whistleblower is an employee, he/she cannot be punished, dismissed or subjected to discriminatory measures for having made a report. Therefore, any direct or indirect reprisal against an employee who has made a report will not be tolerated.

In the event of disciplinary action or dismissal related to the exercise of the right to report, the whistleblower may refer the matter to the industrial tribunal.

Whistleblower protection only applies when the whistleblower has acted in good faith and without self-interest, as indicated above, without seeking to harm the Group.

Abuse, i.e., use of the whistleblowing system in bad faith, may expose the perpetrator to disciplinary sanctions and legal proceedings.

Bad faith consists of using the system to report facts that the person knows to be false or to make defamatory allegations against a third party, with the intention of causing harm or in the hope of obtaining an undue advantage.

Misuse of the whistleblowing mechanism may expose the perpetrator to various penalties, including:

- disciplinary proceedings, which may result in dismissal for misconduct depending on the seriousness of the allegations;
- criminal prosecution for a false accusation (punishable by five years' imprisonment and a fine of €45,000 in France), breach of trust (punishable by three years' imprisonment and a fine of €375,000), and/or deletion or alteration of computer data (punishable by three years' imprisonment and a fine of €100,000), etc.;
- civil liability towards the victim of the false accusation.

WHAT ABOUT CONFIDENTIALITY?

The internal whistleblowing procedure guarantees the confidentiality of the whistleblower's identity, the identity of the person reported and the information collected.

Information that could identify the whistleblower may only be disclosed to judicial authorities with the whistleblower's consent.

Once the validity of the report has been established, information that could identify the person concerned may only be disclosed to the judicial authorities.

Any other disclosure is prohibited.

Anyone who becomes aware of this information during the whistleblowing procedure is subject to a duty of confidentiality.

TO WHOM SHOULD THE REPORT BE MADE?

Choosing the reporting procedure: internal or external

The law provides for two ways in which a report can be made: proceeding with an **internal report** or an **external report**.

You can choose the channel that seems most appropriate, particularly in terms of the effective, impartial and confidential handling of the report:

- Internal reporting involves contacting the company concerned by the facts.
- External reporting involves contacting the relevant authorities.

It is possible to submit an external report to the relevant authorities either directly or after making an internal report.

To benefit from whistleblower protection, public disclosure (e.g., to the media) can only be considered after an external report has been made.

Internal reporting

The option of making an internal report is available to persons interacting with the company concerned, such as employees, corporate officers and third-party stakeholders.

Thus, individuals who, in the course of their professional activities, have obtained information relating to facts that have occurred or are likely to occur in the company concerned may report this information internally, in particular when they believe that the breach can be effectively remedied through this channel and that they are not at risk of reprisals.

External reporting

It is possible to submit an external report, either after making an internal report or directly, at your discretion, to:

- **one of the relevant authorities** listed in the appendix to Decree No. 2022-1284 of 3 October 2022, chosen according to the subject matter of the report (Appendix 1 of this procedure)
For example, for reports concerning individual and collective labour relations and/or working conditions, the designated authority is the Directorate-General for Labour. In matters of employment and vocational training, it is the General Delegation for Employment and Vocational Training, and for matters relating to discrimination, it is the Defender of Rights.
Other examples: for reports concerning the activities of the Ministry of Defence, the General Inspectorate of the Armed Forces; for reports concerning acts of corruption, it is the French Anti-Corruption Agency.
- **the Defender of Rights**, who, depending on the case:

- *Refers the whistleblower to the relevant authorities to handle the report;*
 - *Handles the report within its own areas of competence: children's rights, discrimination, ethics of persons engaged in security activities, and relations with public services.*
- **the judicial authority:**
For example: to the Public Prosecutor if the whistleblower is considering reporting a crime or offence.
 - **to an institution, body or a competent agency of the European Union** to collect information on breaches falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019
For example: referral to the European Anti-Fraud Office concerning fraud affecting the Union budget.

Public disclosure

This refers to making your report public, particularly through the media. Such disclosure is only possible under certain conditions provided for by law in order to qualify as a whistleblower.

COLLECTION OF INTERNAL REPORTS

Who to report to

Whistleblowers should send their reports to the Ethics Officer at the following email address:

referent.ethique@groupeginger.com

This email address can only be accessed by the Ginger Group Ethics Officer.

The Ethics Officer is the Group Human Resources Director.

Content of the report

In order to be processed, all reports must:

- be written in French or English;
- with regard to identity, the whistleblower may choose to disclose his/her identity or remain anonymous. In this case, their attention is drawn to the fact that:
 - anonymous reports are examined with caution in order to avoid the risk of malicious reporting;
 - investigations may be more time-consuming;
 - it is impossible to ensure their protection as a whistleblower since their identity is not known.

At any time during the processing of the report, the author of the report may waive anonymity.

- indicate the identity and functions of the person who is the subject of the report;
- state the facts reported;
- provide any information or documents that may support the report and the seriousness of the facts reported.

This information will then enable the Ethics Officer to analyse and investigate the facts disclosed.

Handling of the report

Receipt of the report

Upon receipt of the report via the designated email address, the Ethics Officer shall:

- send an acknowledgement of receipt of the report within seven days;
- inform the whistleblower of the manner in which they will be informed of the action taken in response to their report;

The Ethics Officer may decide not to inform the person targeted by the report upon receipt of the report if he/she has reliable and verifiable evidence, in order to prevent the destruction of evidence relating to the report.

Any person who is the subject of a report filed under the internal whistleblowing procedure is presumed innocent until the allegations against them have been established.

Upon receipt of the report, the Ethics Officer has one month to confirm to the whistleblower that his/her report has been received and to begin the investigation process.

Upon receipt of the report, the Ethics Officer has a maximum of three months to process the report.

The Ethics Officer shall take all necessary measures to protect the identity of the person making the report, as well as the identity of the persons reported and the nature of the facts.

The Ethics Officer may only refer the matter to the legal representative of the company where the report was made.

Reports are treated with complete confidentiality, as are any subsequent investigations and reports, subject to obligations arising from the law or applicable legal proceedings.

Analysis of the report

Upon receipt of the report, the Officer:

- analyses the seriousness of the alleged facts and the eligibility of the report;
- carries out additional checks where necessary;
- after examining the seriousness of the facts alleged and the accuracy of the information provided, takes a decision on how to handle the report, initiates an investigation and classifies the facts.

Investigation procedure for handling reports

The Ethics Officer lists the actions to be taken and organises an internal investigation, such as a search for evidence, IT searches and interviews with individuals, to determine the reality and materiality of the reported facts.

If necessary, discussions may be organised with the whistleblower, ensuring that their identity remains confidential.

The Ethics Officer will draw up an investigation report.

Resolution – Follow-up on the report

After the Ethics Officer has reviewed the report, the whistleblower will be informed within three months of acknowledgement of receipt of the progress made in handling their report. This information will include:

- the investigative measures taken to establish the accuracy of the facts,
- where applicable, the remedial measures implemented.

EXTERNAL REPORTING: REFERRAL TO AN AUTHORITY DESIGNATED BY LAW

The whistleblower may refer the matter to an external authority. It is not necessary to have first raised the matter internally.

The law has established a list of authorities that can be referred to by whistleblowers, known as external authorities. The list of external authorities is included in the appendix to this procedure.

External authorities are required to publish on their websites the rules of procedure they apply and the means by which they can be contacted.

The procedure may vary slightly from one authority to another, but it must at least provide the following information:

- the scope of the authority's powers;
- who to send the report to (postal address, telephone number and email address);
- what information to provide;
- what precautions must be taken to ensure the confidentiality of the report;
- how the report will be handled (by post, email, etc.);
- the contact details of the Defender of Rights.

The procedure established within the authority must include the following guarantees:

- the possibility of reporting in writing or orally;
- the issuance of an acknowledgement of receipt of the report within seven days;
- a guarantee of the integrity and confidentiality of the data collected (identity of the whistleblower and the person reported);
- the handling of the report by staff with sufficient authority and resources;
- written communication of information on the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to rectify the matter reported;
- response timeframes.

Response timeframes vary depending on the authority involved and the nature of the case.

DATA PROCESSING POLICY

What data are processed?

Only data required for fact-checking may be processed.

This includes:

- where applicable, the identity, roles and contact details of the whistleblower;
- the identity, roles and contact details of the persons reported;
- the identity, roles and contact details of the persons involved in collecting or processing the report;
- the facts reported;
- the information gathered in the course of verifying the reported facts;
- the report on the verification operations;
- the action taken in response to the report.

The person who is the subject of a report under the internal whistleblowing procedure may not under any circumstances obtain, based on their right of access, information concerning the identity of the person who made the report.

Confidentiality may be waived in the following cases:

- disclosure of the identity of the whistleblower with their consent;
- disclosure of the person reported once the report has been established as well-founded;
- transmission to the judicial authorities.

Retention period

The data retention period depends on the status of the report:

- Reports received are retained until a final decision is made on the action to be taken.
- When a final decision is taken on how to respond to the report:
 - The report is either inadmissible because it does not fall within the scope of the internal whistleblowing procedure: the data is stored for a period of three months from the date on which the whistleblower is informed of the inadmissibility of their report, in order to deal with any questions the whistleblower may have regarding this decision,
 - Or, the report is admissible and is dismissed without further action or gives rise to non-disciplinary or non-judicial action: the data is kept for one year from the date of the decision, for the following purposes:
 - to protect the various parties involved (the whistleblower, the facilitator, and the person mentioned or targeted in the report) against the risk of reprisals.
 - to enable any further investigations.
 - to provide evidence of the handling of the report in the event of litigation or subsequent checks on the compliance of the whistleblowing process. (audit or authority),

- Or, the report is admissible and gives rise to disciplinary or legal proceedings against the person reported or against the author of a wrongful report: the data is retained until the end of the proceedings or until the time limit for appealing against the decision has expired.

Beyond these retention periods, the data is anonymised or deleted.

Data destruction and security measures

The Ethics Officer shall take all necessary measures to preserve the security and confidentiality of the data, both during its collection, processing and storage and during its communication (e.g., restricted access on a secure server, safe, etc.).

If the report falls within the scope of the whistleblowing procedure, the Ethics Officer shall destroy all data communicated within the following time limits:

- Personal data collected that is not followed by disciplinary or legal proceedings shall be destroyed or archived, after anonymisation, within two months of the end of the admissibility analysis or the closure of the verification operations;
- Where disciplinary proceedings or legal proceedings are brought against the person reported or the author of a wrongful report, the data relating to the report shall be destroyed by the Ethics Officer after the disciplinary or legal proceedings have been closed.

Personal data

Any personal data communicated by a whistleblower in accordance with this whistleblowing procedure will be processed in accordance with the applicable legal provisions on the protection and processing of personal data.

This data is collected for the purpose of complying with the Sapin II law and, more generally, with the legal obligations applicable to the GINGER Group. It will be stored in a computerised file and may be transmitted to the competent administrative and judicial authorities.

The retention period for this data is limited to the period specified in this Procedure.

The whistleblower or the person reported may access the data concerning them and request that it be corrected or deleted if it is inaccurate, incomplete, ambiguous or out-of-date.

The request must be made to the Ethics Officer responsible for handling the report using the designated email address.

The whistleblower or the person reported may be assisted by any person of their choice within the company at all stages of the procedure.

FOLLOW-UP ON REPORTS

In order to assess the effectiveness of the whistleblowing procedure, the person responsible for handling reports shall establish annual statistics on the receipt, handling and follow-up of reports.

This annual statistical follow-up shall show the number of reports received, cases closed, cases that have led or are leading to an investigation, and the number and type of measures taken during and after the investigation, such as precautionary measures, initiation of disciplinary or legal proceedings and sanctions imposed.

PUBLICISING THE INTERNAL WHISTLEBLOWING PROCEDURE

It is essential that employees and external stakeholders are aware of the whistleblowing procedure in order for it to be effective. All GINGER staff are informed of the existence of this mechanism and the present procedure through internal communications and the presentation of the procedure on the intranet.

Third parties are informed of the existence of the procedure through information published on the institution's website at www.groupeginger.com

KEY POINTS

- ☒ This whistleblowing procedure has been set up in accordance with the Sapin II Law.
- ☒ It is not an obligation but an additional option offered to employees and stakeholders.
- ☒ The procedure defines the methods for reporting and the handling of reports by employees or stakeholders.
- ☒ Whistleblowers will not be subject to any sanctions if they report in good faith, as described in this procedure. Barring exceptional circumstances, their identities will remain confidential throughout the handling of the report.
- ☒ Misuse of the whistleblowing procedure may result in sanctions for the person making the report.

Appendix 1

1. Public procurement:
 - French Anti-Corruption Agency (AFA), for breaches of integrity;
 - Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF), for anti-competitive practices;
 - Competition Authority, for anti-competitive practices;
2. Financial services, products and markets, and prevention of money laundering and terrorist financing:
 - Financial Markets Authority (AMF), for investment service providers and market infrastructures;
 - Prudential Supervision and Resolution Authority (ACPR), for credit institutions and insurance organisations;
3. Product safety and compliance:
 - Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF);
 - Central Arms and Explosives Service (SCAE);
4. Transport safety:
 - Directorate-General for Civil Aviation (DGAC), for air transport safety;
 - Bureau of Investigation and Analysis for Land Transport (BEA-TT), for land transport safety (road and rail);
 - Directorate-General for Maritime Affairs, Fisheries and Aquaculture (DGAMPA), for maritime transport safety;
5. Environmental protection:
 - General Inspectorate for the Environment and Sustainable Development (IGEDD);
6. Radiation protection and nuclear safety:
 - Nuclear Safety Authority (ASN);
7. Food safety:
 - General Council for Food, Agriculture and Rural Areas (CGAAER);
 - National Agency for Food, Environmental and Occupational Health and Safety (ANSES);
8. Public health:
 - National Agency for Food, Environmental and Occupational Health and Safety (ANSES);
 - National Public Health Agency (Santé publique France, SpF);
 - High Authority for Health (HAS);
 - Agency for biomedicine:
 - French Blood Establishment (EFS);
 - Compensation Committee for Victims of Nuclear Tests (CIVEN):
 - General Inspectorate of Social Affairs (IGAS):
 - National Institute of Health and Medical Research (INSERM):
 - National Council of the Order of Physicians, for the practice of the medical profession;
 - National Council of the Order of Physiotherapists, for the practice of the profession of physiotherapist
 - National Council of the Order of Midwives, for the practice of the profession of midwife;
 - National Council of the Order of Pharmacists, for the practice of the profession of pharmacist;
 - National Council of the Order of Nurses, for the practice of the nursing profession;
 - National Council of the Order of Dental Surgeons, for the practice of the profession of dental surgeon;
 - National Council of the Order of Podiatrists, for the practice of the profession of podiatrist
 - National Council of the Order of Veterinarians, for the practice of the profession of veterinarian;
9. Consumer protection:
 - Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF)
10. Protection of privacy and personal data, network and information system security:
 - National Commission for Information Technology and Civil Liberties (CNIL):
 - National Information Systems Security Agency (ANSSI);
11. Breaches affecting the financial interests of the European Union:
 - French Anti-Corruption Agency (AFA), for breaches of integrity;
 - Directorate-General for Public Finances (DGFIP), for value added tax fraud:
 - Directorate-General for Customs and Indirect Taxation (DGDDI), for customs duty fraud, anti-dumping duties and similar duties
12. Breaches relating to the internal market:
 - Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF), for anti-competitive practices;
 - Competition Authority, for anti-competitive practices and state aid;
 - Directorate-General for Public Finances (DGFIP), for corporate tax fraud;
13. Activities conducted by the Ministry of Defence
 - General Control of the Armed Forces (CGA);
 - College of Inspectors General of the Armed Forces;
14. Public statistics:
 - Public Statistics Authority (ASP);
15. Agriculture:
 - General Council for Food, Agriculture and Rural Areas (CGAAER);
16. National education and higher education:
 - National Education and Higher Education Ombudsman:
17. Individual and collective labour relations, working conditions:
 - Directorate-General for Labour (DGT);
18. Employment and vocational training:
 - General Delegation for Employment and Vocational Training (DGEFP);
19. Culture:
 - National Council of the Order of Architects, for the practice of the profession of architect;
 - Council of Auction Houses, for public auctions;
20. Rights and freedoms in relations with State administrations, local authorities, public institutions and bodies entrusted with a public service mission:
 - Defender of Rights;
21. Best interests and rights of the child:
 - Defender of Rights;
22. Discrimination:
 - Defender of Rights;
23. Ethics of persons engaged in security activities:
 - Defender of Rights.