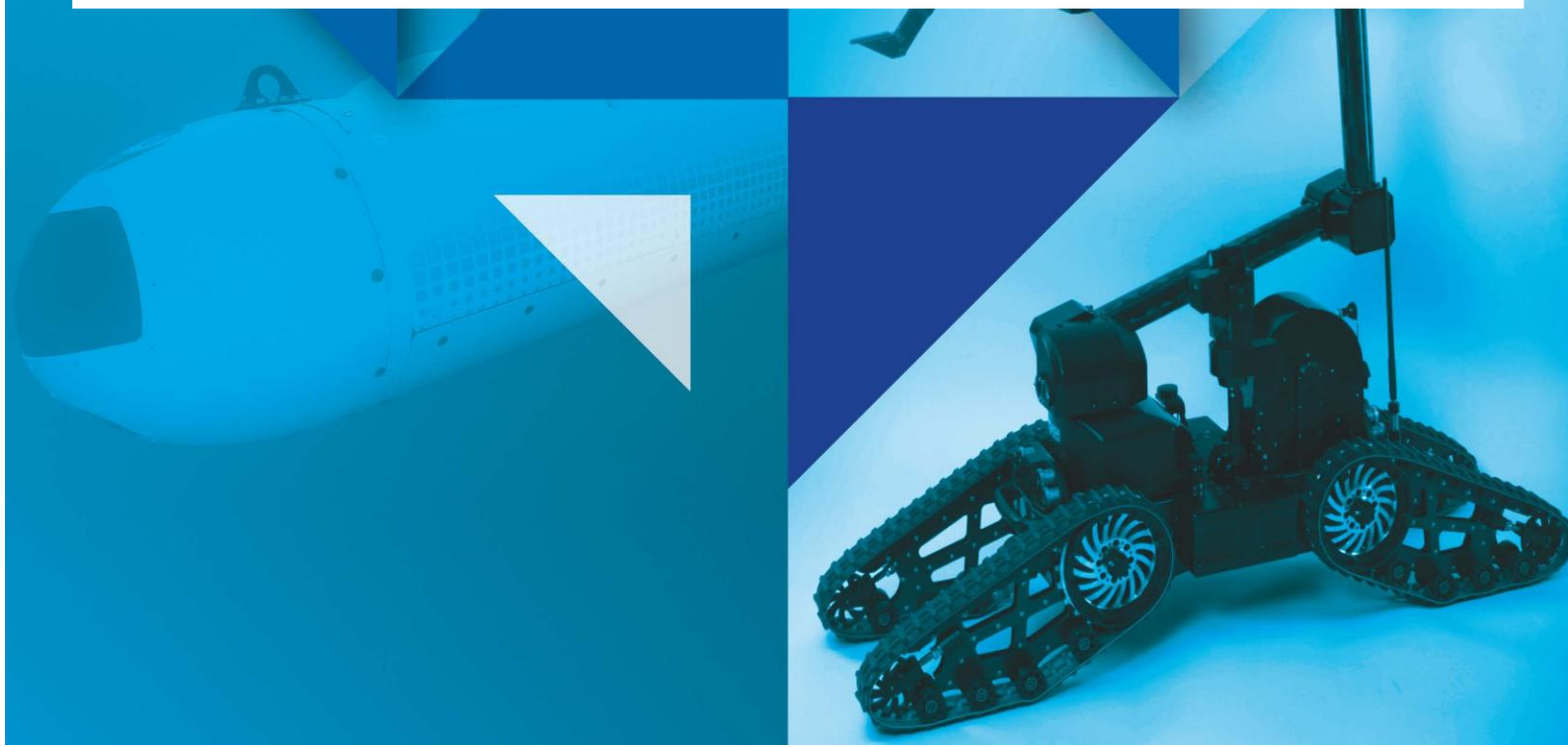
GROUPE Gorgé

INTERNAL WHISTLEBLOWING POLICY



CONTENTS

1. OBJECTIVES AND SCOPE OF THE WHISTLEBLOWING POLICY

1.1 A SINGLE WHISLTEBLOWING POLICY FOR TWO TYPES OF REPORTING

In compliance with the Sapin II Law[1], this policy responds to the following dual objective:

1. **Receiving anti-corruption alerts**[2]: For the prevention and detection of corruption and influence-peddling that the group may face in France or abroad, any employee in the group's subsidiaries may report to a Groupe Gorgé Anti-Corruption Officer any conduct contrary to the Groupe Gorgé Anti-Corruption Code of Conduct[3] or, as applicable, to the anti-corruption code of conduct adopted by Groupe Gorgé subsidiaries.

2. **Receiving general alerts of very serious offenses**[4]: Any staff member and any external or occasional employee (intern, temp, service provider, subcontractor) of the French subsidiaries with more than 50 Groupe Gorgé employees may report any crimes, misdemeanors, serious and obvious violations of applicable international regulations, laws or rules, or serious threats or harm to the public interest.

The term "employee" used hereinafter includes any staff member of the group and any external or occasional employee.

Groupe Gorgé subsidiaries are invited to adopt this whistleblowing policy if they do not already have one. It will be appended to their internal rules after consultation with the IRP and distributed internally to all employees by any means (posting, mailing, intranet, etc.).

This policy is a supplement to any other existing policies in the group's subsidiaries. It is simply an additional option offered to every employee.

1.2 DEFINITION OF A WHISTLEBLOWER

The status as a protected Whistleblower will apply if the Whistleblower meets all of the following criteria:

- He or she is a ***natural person***;
- the Whistleblower has ***personal knowledge*** of the facts that he or she is reporting: he or she is not reporting facts alleged by others;
- the Whistleblower is acting ***impartially***: he or she is not gaining any benefit or being compensated by anyone in exchange for his or her actions;

[1] Law 2016-1691 of December 9, 2016, known as the "Sapin II Law"
[2] Pursuant to Article 17 of the Sapin II Law
[3] Groupe Gorgé's Anti-Corruption Code of Conduct is available on the group's website at www.groupe-gorge.com
[4] Pursuant to Article 6 of the Sapin II Law

- He or she is acting in ***good faith***: at the time of making a report, the facts reported must show all appearances of an act of corruption such that, after the fact, the Whistleblower cannot be accused of attempting to cause harm to others.
  As a reminder, anyone making false accusations is subject to prosecution (see Chapter 4);
- the facts reported are ***serious***; they constitute:
  - a violation of the Groupe Gorgé Anti-Corruption Code of Conduct or that of one of its subsidiaries,
  - a crime, a misdemeanor,
  - a serious and obvious violation of a commitment duly ratified or approved by France, a unilateral act by an international organization taken on the basis of such a commitment, the law, or regulations; or
  - a serious threat or harm to the public interest;
- the Whistleblower cannot reveal any information covered by National Defense secrecy, doctor-patient confidentiality, or attorney-client privilege.

Only a person meeting the above criteria may be qualified as a **whistleblower** and therefore eligible for the Whistleblower protection scheme as set forth by law (see Chapter 4).

The alert must be made in good faith, based on facts of which the Whistleblower has personal knowledge.

The alert is not about an individual or collective labor dispute: the alert is general in scope, in the interest of the common good and ethics.

Whistleblowing is an option open to every citizen to freely exercise his or her responsibility to report on crimes and misdemeanors or serious threats to health, public safety, or the environment; it is not an obligation.

1.3 OFFICERS AND ETHICS COMMITTEE

The Officer(s) is (are) tasked with receiving and handling alerts sent to the alert email **compliance@groupe-gorge.com**.

The Chairman and Chief Executive Officer of Groupe Gorgé has appointed the Chief Legal Officer of Groupe Gorgé and the Chief Financial Officer as Officers. Appointing two people limits the risks of any delay in processing in case of the absence of either Officer. These two individuals have been appointed for their competence, their authority, and the sufficient resources they have to properly carry out this mission.

On the basis of the reports received, the Officers bring together an **Ethics Committee** to decide on how to handle the reports, implement an investigation, and consider the facts. This Committee may be composed of:

- the HRD of the relevant subsidiary;
- an internal or external IT expert;
- Officers from the group's other subsidiaries
- an attorney ;
- any expert internal or external to the group whose expertise is required to handle an alert;
- in the event of special challenges (importance of the issues, individuals involved, etc.), referral to the Executive Management of the relevant subsidiary and to the Chairman & CEO of Groupe Gorgé is organized.

The geometry of the resulting Ethics Committee will depend on the alerts and expertise required on a case-by-case basis. The committee may not include any person in a position of conflicting interest with a given alert.

Every member of the Ethics Committee will be expected to sign an ethics charter which will state (i) the general principles governing whistleblowing, (ii) the procedures for conducting internal investigations, and (iii) the obligations of confidentiality, neutrality, and impartiality to be respected in all circumstances by Committee members.

The Ethics Committee will handle the alerts relayed by the Officers.

2. HOW TO ISSUE AN ALERT

2.1 ESCALATION PROCEDURE

The Sapin II Law stipulates an **escalation procedure, in two stages**:

- first, the Employee must notify his or her immediate superior, or employer, of the alert, or use the Officers' email address, or another reporting channel in place within his or her company;
- second, he or she may send his or her alert to third parties if the alert is not handled within a reasonable time frame or in the event of blatant urgency.

> *The protection of a Whistleblower who is a staff member of the group is dependent on compliance with this two-stage procedure.*

2.1.1 REPORTING TO THE INTERNAL OFFICER

In addition to the other reporting channels that may exist within each subsidiary, the Whistleblower makes his or her report to the internal Officers appointed by the group, who can be reached at the following email address:

compliance@groupe-gorge.com

This email can only be viewed by the Officers of Groupe Gorgé.[5]

Before issuing an alert, any Employee may – if desired – speak to his or her immediate supervisor or to any individual named as a contact in the Anti-Corruption Code of Conduct of the group or its subsidiary. This contact's duty is to guide and advise the Whistleblower.

2.1.2 WHISTLEBLOWING STAGE TWO

a) If his or her alert is not handled within a reasonable time frame, the Employee may refer the matter to the administrative or judicial authorities, or to a professional association.
b) If the alert is not handled within three months of its reporting by one of the bodies to which it has been referred, the report may be made public.
c) In the event of serious and imminent danger, or if there is a risk of irreversible damage (to health, the environment, etc.), the report may be made directly to the judicial authorities, administrative authorities, or professional associations. It may also be made public.

2.2 CONTENTS OF THE ALERT

In order to be handled, every alert must:

- be written in the French or English language;
- include the identity and contact information of the Whistleblower;

The Whistleblower must state his or her identity. This prevents false or baseless accusations and makes it possible to request information from the Whistleblower, as applicable. His or her identity will be protected by the Officers and the Ethics Committee.

However, the Whistleblower may, if he or she wishes, remain anonymous if (i) the facts are proven to be serious and (ii) the factual elements of the alert are sufficiently detailed.

[5] It might also be accessible to IT department staff who maintain IT services, in the event of an IT problem with the group's servers.

- state the identity and duties of the individual reported on;
- state the facts reported;
- supply all information or documents that substantiate the report and the seriousness of the facts reported.

The reporting must be precise and accompanied by evidence (correspondence, reports, accounting records, etc.).

These items will allow the Officers and Ethics Committee to analyze and investigate the facts disclosed.

3. HOW AN ALERT IS HANDLED

3.1 RECEIPT OF AN ALERT

When the alert is received via the dedicated email, an Officer:

- will send the Employee an acknowledgment of the report within a reasonable time frame;
- will inform the Employee of the reasonable and foreseeable period within which his or her report will be handled;
- will tell the Employee what procedures will be used to notify him or her of the response given to his or her report.

3.2 ANALYSIS – MAKEUP OF THE ETHICS COMMITTEE

Upon receipt of a report, the Officers:

- analyze the seriousness of the alleged facts and the *prima facie* admissibility of the alert;
- proceed, as applicable, with basic fact-checking;
- after reviewing the seriousness of the alleged facts and the accuracy of the information given, the Officers form an Ethics Committee to decide on how to handle the alert, implement an investigation, and consider the facts.

3.3 INTERNAL INVESTIGATION

- The Ethics Committee lists the actions to be taken and expedites an internal investigation (evidence gathering, computer searches, interviews, etc.) to determine the reality and materiality of the facts reported.

- Where applicable, discussions preserving the confidentiality of the Whistleblower's identity may be organized with him or her.
- The Ethics Committee informs the persons named in the report, except in cases of interim measures for evidence-gathering to be implemented in advance.
- The Ethics Committee decides on the advisability of either drafting a written investigation report or providing an oral summary of the investigation.

3.4 RESOLUTION - ACTIONS TAKEN IN RESPONSE TO THE ALERT

Following a review of the alert by the Ethics Committee, regardless of the action taken, the Ethics Committee's decision will be formalized in a document that will be sent (in full or in part) to the Whistleblower by the Officers.

3.5 FUNDAMENTAL PRINCIPLES OF HANDLING ALERTS

All reports will be handled by the Officers and the Ethics Committee in keeping with the following fundamental principles:

- confidentiality;
- protection of the Whistleblower;
- presumed innocence of the persons named in the alert;
- respect of privacy;
- doctor-patient confidentiality, National Defense secrecy, and attorney-client privilege.

3.6 RETENTION OR DESTRUCTION OF MATERIAL ON FILE

One of several different scenarios may arise:

1/ If the alert does not fall within the scope of the internal whistleblowing policy, then all data that have been disclosed and that identify the Whistleblower and the person implicated will be destroyed by the Officers immediately;

2/ If the alert does fall within the scope of the internal whistleblowing policy, the Officers will destroy all disclosed data within the following time frames:

- if the alert is followed by disciplinary proceedings, or judicial proceedings are undertaken: destruction of the material on file that identifies the Whistleblower and the person implicated, promptly after the disciplinary or judicial proceedings are closed,
- if no action is taken on the alert: destruction of the material on file that identifies the Whistleblower and the person implicated, within two months after the end of the admissibility analysis or the verification.

In every case, the Officers retain the anonymized elements establishing the number of and basis for the alerts, and the actions taken in response. Where applicable, all of these items will be used to update the group's anti-corruption program.

4. PROTECTION OF THE WHISTLEBLOWER

Pursuant to the Sapin II Law, a Whistleblower who acts in good faith and impartially cannot be disqualified from a recruitment process, access to an internship, or professional training; no staff member can be sanctioned, terminated, or discriminated against for having issued an alert.

Therefore, no reprisals will be tolerated, whether direct or indirect, against an Employee who has issued an alert.

Of course, Whistleblower protection is only to be applied if the Whistleblower acted in good faith and impartially, as stated above, without seeking to harm the group.

Any abuse of the whistleblowing policy can result in various sanctions against the perpetrator, particularly:

- disciplinary proceedings up to and including termination for misconduct, depending on the severity of the alleged facts;
- criminal proceedings for the criminal offense of false accusation (punishable by five years in prison and €45,000 in fines in France), breach of trust (punishable by three years in prison and €375,000 in fines), and/or deletion or alteration of computer data (punishable by three years in prison and €100,000 in fines), etc.;
- civil liability toward the victim of the false accusation.

5. CONFIDENTIALITY AND MANAGEMENT OF PERSONAL DATA

5.1 CONFIDENTIALITY MANAGEMENT

As confidentiality is one of the fundamental principles in handling an alert, you are reminded that the Whistleblower's identity will not be disclosed to the person(s) implicated in the alert, without the Whistleblower's agreement.

When handling an alert, only the following information will be recorded:

- the identity, duties, and contact information of the Whistleblower, the persons implicated in the alert, and the persons involved in receiving or handling the alert;
- the facts reported;
- the information gathered during the fact-checking process;
- the summary of the fact-checking operations;
- the actions taken in response to the alert.

The receipt, handling, and classification of an alert will be treated confidentially, subject to the obligations under the law or applicable judicial proceedings. Specific procedures have been put in place to guarantee strict confidentiality of: (i) the Whistleblower's identity; (ii) the identity of the persons implicated in the alert; and (iii) the information gathered by all recipients of the report. These mechanisms include in particular the establishment: (i) of an email address with restricted access for the Officers, (ii) a locally-hosted storage (or cloud) space whose server access is secured, (iii) an ethics charter signed by the members of the Ethics Committee (including the Officers) informing them of the sanctions applicable in the event of a breach of confidentiality; (iii) the confidentiality agreements with any and all third parties if the fact-checking or handling of an alert requires external expertise; and (iv) the procedures for destroying or archiving the data.

Confidentiality may be removed in the following cases:

- disclosure of the Whistleblower's identity, with his or her consent;
- disclosure of the person implicated in the alert once the alert has been proven legitimate;
- referral to the judicial authorities.

5.2 PERSONAL DATA

All personal data shared by an Employee under this internal whistleblowing policy will be handled in keeping with the laws applicable to personal data protection and processing.

These data are collected for the purpose of compliance with the Sapin II Law, and more generally with the legal obligations applicable to Groupe Gorgé. They will be saved in an electronic file, and may be shared with the Ethics Committee and the competent administrative and judicial authorities.

The retention period for these data is limited to the period mentioned in this policy.

At any time, the Whistleblower and the person who is the subject of the alert may access the data about them and request that they be corrected or deleted if they are inaccurate, incomplete, questionable, or out of date. Such requests are to be made to the Officers, via the email address compliance@groupe-gorge.com, with the understanding, however, that the person who is the subject of an alert cannot in any event obtain information about the Whistleblower.

6. KEY POINTS

- **This internal whistleblowing policy is established pursuant to the Sapin II Law.**
- **It is a supplement to any other policies applicable in the group's subsidiaries. It is not an obligation, but an additional option offered to Employees.**
- **The policy defines the procedures for launching and handling an alert made by an Employee.**
- **The Whistleblower does not incur any sanction for an alert made in good faith, as described in this policy. Unless otherwise specified, his or her identity will remain confidential throughout the alert handling process.**
- **Any abuse of the whistleblowing policy can result in sanctions against the perpetrator.**