HIGHCO GROUP'S WHISTLE BLOWING SYSTEM IN FRANCE

HighCo

Preamble

In 2018, the HighCo Group adopted an anti-corruption code of conduct and an internal whistleblowing system, in accordance with the “Sapin 2” Act of 9 December 2016.

Since the “Waserman” Act of 21 March 2022 and its implementing decree of 3 October 2022 strengthened the protection of whistle-blowers, the coming into force of these new texts have led HighCo to review its internal whistle-blowing system.

The HighCo Group has opted to implement a single technical system for collecting these reports for all its French subsidiaries

VERSION	DATE	MODIFICATION
V1	2018	Initial version
V2	2021	Links updated to access the whistle-blowing system at www.highconnect.fr
V3	2023	Update of the Waserman Act of 21/03/22 and implementing decree of 03/10/22

TABLE OF CONTENTS

1. Who can be a whistle blower?

Any natural person as defined in Article 6-I of the Act No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (the "Sapin II Act"), and in particular members of staff, shareholders, members of administrative, management or supervisory bodies, external and/or occasional employees, co-contractors and sub-contractors.

In order to process the reports submitted under this system, the HighCo group has set up an Ethics Committee comprising 3 members, whose respective functions are Legal Director, Chief Financial & CSR Officer, Human Resources Director.

2. What can be reported?

Acts that have occurred or are very likely to occur and which are defined as acts that may be reported by a whistle-blower:

- Any breach of the law, of an international commitment
- Any attempt to conceal this breach
- Any serious threat or harm to the public interest

The whistle-blowing system thus makes it possible to report acts in the following areas:

- Any breach of a group Charter or Code of Conduct;
- Corruption, anti-competitive practises, money laundering;
- Accounting, financial or banking violations;
- Discrimination, harassment;
- Health and safety in the workplace;
- Protection of public health;
- Environmental protection;
- Protection of privacy, personal data and information systems security;
- Consumer protection, product safety and conformity;
- Others.

The list is not exhaustive but only information of an unlawful nature or detrimental to the general interest may be reported, and this excludes for example simple malfunctions within a company

Furthermore, the whistle-blowing system and the legal protection of whistle-blowers does not apply when a report relates to facts, information and documents the disclosure of which is prohibited by Law and relating to classified national defence information, medical confidentiality, the secrecy of judicial deliberations, the secrecy of judicial investigations or lawyer-client privilege.

3. What is the status and protection of whistle-blowers?

Five conditions must be met in order to be able to submit a report (see Article 6-I of the "Sapin II Act"):

1. The whistle-blower must be a natural person;
2. The information must have been obtained in a professional context; if the information was obtained outside a professional context, the whistle-blower must have been personally aware of the facts. In this case, a whistle-blower cannot simply report acts observed by someone else.
3. The whistle-blower must act without any direct financial compensation; the whistle-blower must not benefit from a financial advantage resulting directly from their report.
4. The whistle-blower must act in good faith; they must not act with the intention of causing harm and must be sure that the acts they are reporting actually happened, in light of the information available to them. In this respect, they are advised to have concrete evidence of the facts reported (emails, documents, accounting information, etc.),
5. Disclose the elements mentioned in Article 2 above.

The whistle-blower may have access to one or more trusted persons. These trusted persons benefit from the protection granted by whistle-blower status and the rights relating thereto.

The following are therefore considered to be protected third parties (see Article 6.1 of the "Sapin II Act"):

- A facilitator: i.e. a natural person (e.g. a colleague) or a non-profit legal entity (e.g. an association under the Act of 1901) that helps the whistle-blower to report or disclose information;
- A natural person (e.g. a relative) in connection with a whistle-blower and who risks suffering retaliation;
- An entity (e.g. a company) controlled by the whistle-blower or for which they work or have professional links.

The person concerned may, after making a report, submit a request to the Défenseur des Droits (Rights Advocate) for an opinion (or certification) as to whether they are eligible for whistle-blower status.

A person who misuses the system or who acts in a wilfully slanderous manner is liable to disciplinary sanctions. The person is also liable for criminal prosecution and/or civil suits.

When these criteria are met, the whistle-blower benefits from certain statutory guarantees (see Article 10-1 of the "Sapin II Act"):

- Absence of criminal liability in the event of disclosure of a secret protected by law (e.g. secrecy of correspondence). However, this does not apply to secrets relating to: classified national defence information, medical confidentiality, the secrecy of judicial deliberations, the secrecy of judicial investigations or lawyer-client privilege.
- Absence of criminal liability in the event of embezzlement, misappropriation or concealment of documents or any medium containing the information of which they have knowledge and which they disclose.
- Absence of civil liability, particularly for the person who publicly disclosed information. They will not be accountable for the damage caused.
- They may not be dismissed, disciplined, discriminated against or subjected to retaliation as a result of the whistle-blowing report.

The Law provides for:

- A one-year prison sentence and a fine of €15,000 for any person obstructing in any way the transmission of an internal report to the company or to the judicial, administrative or professional authority.
- A fine of €60,000 for any person (natural or legal) who attacks a whistle-blower through dilatory or abusive process. At the time of the proceedings, the whistle-blower may be awarded financial aids if their economic situation has seriously deteriorated. The person initiating the action shall also be ordered to pay damages to the whistle-blower. The sentencing decision may be posted publicly or distributed.
- A two-year prison sentence and a €30,000 fine against any person (natural or legal) who discloses confidential information relating to the whistle-blower.
- A three-year prison sentence and a €45,000 fine against any person who attempts to discriminate against a whistle-blower, their facilitators or any person in connection with the whistle-blower.
- The possibility for the court to impose an obligation to deposit funds in the whistle-blower's professional training account.

Any company employee who is guilty of any one of these offences is liable for disciplinary sanctions and may be officially reported to the competent authorities.

4. What guarantees are given to whistle-blowers (confidentiality and GDPR)?

All data collected as part of this whistle-blowing procedure will be treated as confidential, whether they concern:

- The identity of the whistle-blower,
- The facts in the report
- Witnesses concerned by the report
- Or persons implicated in the report.

All necessary precautions will be taken to keep these data secure.

- For this purpose, the persons in charge of collecting or processing reports are bound by a strict non-disclosure obligation,
- Personal data collected in the course of this whistle-blowing procedure are processed in accordance with the provisions of the General Data Protection Regulation (GDPR).

5. How and to whom should the report be sent?

The law provides for two means of whistle-blowing: either by submitting an internal report or an external report.

Internal reporting is only possible if you obtain the information concerning the incident in the course of your professional activities. External reporting consists of bringing the report to the attention of an institution designated by law.

OPTION 1: INTERNAL REPORTING

1. You can use the dedicated, secure and confidential email address at your disposal

If you believe that it is possible to effectively remedy the breach internally and that you do not risk retaliation, you may send a report to the following dedicated email address: alerte_highco@nest-avocats.com. This is a secure and confidential external email address that does not go through HighCo's IT network.

In order to guarantee the confidentiality and impartiality of its system, HighCo has entrusted an independent external firm with the task of collecting the reports and carrying out an initial admissibility analysis. This firm is Labrador Ethics & Compliance, in partnership with Nest Avocats, an independent law firm.

If the report is deemed admissible by Nest Avocats, it is sent to the Ethics Committee, which will process it in accordance with paragraph 6 below and its Code of Ethics.

The information to be communicated is as follows:

1. Your surname, first name, position and place of work; you may choose to remain anonymous. However, the obligation for HighCo to provide feedback does not apply when the report is anonymous.

2. The facts that you wish to communicate in a manner sufficiently objective and precise to enable the alleged facts to be checked;

3. An email address if you wish to be informed of the processing of the report if this address is different from the one used for the initial report.

2. You can also choose to write and/or ask your questions directly to a manager in the HighCo group

This person may be:

- Your line manager or the manager above your line manager;
- The Human Resources Manager;
- The Managing Director and/or the Chairman.

They will be required to forward your disclosures to the Group Ethics Committee that will process the report. If you have any questions, you can also put them directly to the Group Ethics Committee in an email sent to the following dedicated address: comite-ethique@notification-highco.com

OPTION 2: EXTERNAL REPORTING

If you do not wish to make an internal report, you may refer the matter directly to the judicial authorities or one of the authorities mentioned in the Decree of 3 October 2022, the list of which is appended to this document, or to the Défenseur des Droits (rights advocate) who will refer you to the appropriate authority. The entire administration is bound by a transmission obligation. So even if you do not select one of the authorities mentioned in the appendix, the administration will forward your report to the appropriate authority.

In particular, you may refer the matter to these external authorities:

- If you believe that an internal report will not remedy the situation internally or if you fear retaliation:
- When a report submitted internally remains unanswered for 3 months following the date of the acknowledgement of receipt or when such a report fails.

6. When can you make your report public?

Public disclosure (e.g. to the media) can only be considered after the report has been submitted to an external authority and is only possible in the following 4 cases:

1. If you have referred the matter to an external authority that has not provided you with an appropriate response within the time indicated,

2. In the event of both serious and imminent danger for reports that do not concern information obtained in a professional context,

3. In the event of imminent or manifest danger to the public interest, particularly in an emergency or when there is a risk of irreversible harm being caused, for reports that concern information obtained in a professional context,

4. If you risk retaliation by referring the matter to an external authority or if the authority does not effectively remedy the situation highlighted in your report, especially when evidence risks being concealed or destroyed or when you have serious reason to believe that the authority has a conflict of interest, is colluding with the perpetrator of the acts reported or involved in perpetrating the said acts.

Discernment is therefore required when deciding whether to disclose the report publicly as there is a risk of losing the benefit of protective provisions.

7. How is the alert processed internally?

- You will receive an acknowledgement of receipt at the email address used to submit your report or at the address chosen by you for correspondence and this within 7 days of submitting your report.
- You will then be informed of the estimated time required to determine whether your report is admissible.
- The Ethics Committee will conduct the necessary investigations to find evidence that proves or disproves the reality of the alleged facts within a reasonable period of time. It may have recourse to an external service provider for this purpose.
- You will be informed of the progress of the procedure, i.e. the measures envisaged or taken to assess the accuracy of the facts within 3 months.
- When it deems the allegations to be founded, the Ethics Committee will use the means at its disposal to remedy the situation.
- The Ethics Committee closes the whistle-blowing case when it finds the allegations to be inaccurate or unfounded, or when the report has become irrelevant.
- You will be informed of this decision in writing.

8. Retention of personal data

Purposes of the processing

The processing of internal whistle-blowing data must be carried out for specific purposes and be justified in light of the organisation's missions and activities. With regard to whistleblowing systems, data processing is carried out in order to:

- Collect and process reports submitted by whistle-blowers concerning the breach of a specific rule;
- Carry out the necessary checks, investigations and analyses;
- Determine the actions to be taken in light of the report;
- Ensure that data subjects are protected;
- Exercise or defend legal rights.

Legal basis for the processing

Each processing purpose must be based on one of the "legal bases" laid down in the regulations. In the context of this processing, the legal basis may be:

- Compliance with a legal obligation incumbent on the organisation, requiring a whistle-blowing system to be implemented (for example, the "Sapin 2" Act)
- The fulfilment of the legitimate interest pursued by the organisation or by the recipient of the data, provided that it does not disregard the interest or the fundamental rights and freedoms of the data subject. This legal basis applies when implementing a whistle-blowing system does not arise out of a legal obligation.

Collection of personal data

Implementation of the Whistle-blowing System is managed by HighCo SA (353 113 566 RCS Aix-en-Provence) who acts as data controller. In the context of a whistle-blowing report, only the data required to pursue the aforementioned processing purposes will be effectively collected and processed. These data include:

- The identity, position and contact details of the whistle-blower;
- The identity, position and contact details of the person(s) about whom a report is made;
- The identity, position and contact details of the persons involved in collecting or processing reports;
- The facts reported;
- The information collected in the course of checking the facts reported;
- The report on checking operations;
- The action taken following the report.

The evidence collected is strictly limited to the scope of the Whistle-blowing System, and must be directly related to the subject-matter of the report. This evidence must not be classified national defence information, information covered by medical confidentiality provisions, the secrecy of judicial deliberations, the secrecy of judicial investigations or lawyer-client privilege.

Personal data retention period

Data relating to a whistle-blowing report may be kept in an active database until the final decision is made as to the follow-up to be given to the report. This decision must be made within a reasonable period of time from the time the report is received. After the final decision on the follow-up to be given

to the report has been taken, the data may be kept in the form of interim archives, for a period strictly proportionate to the processing of the report and to the protection of the whistle-blower, the persons implicated in the report and the third parties mentioned, taking into account the time required for any additional investigations. When disciplinary or litigation proceedings are initiated against an implicated person or the perpetrator of an abusive report, the data relating to the report may be kept by the organisation responsible for managing reports until the end of legal proceedings or until the limitation period for appeals against the decision made is reached. The data may be kept in interim archives for a longer period if the data controller is legally obliged to do so (for example, to meet accounting, social security or tax obligations), or may be kept as evidence with a view to an audit or possible litigation, or for the purpose of carrying out quality audits on whistle-blowing report processing.

Complying with the right to access and rectify personal data

The Group guarantees the rights of any person identified in a whistle-blowing case to access their data and, if said data are incorrect, incomplete, ambiguous or out-of-date, to demand that these data be rectified or deleted. In particular, every person identified in a whistle-blowing case has the right to correct, complete, update, lock or delete any of their personal data that are incorrect, incomplete, ambiguous or out-of-date or if the collection, use, communication or storage thereof is prohibited. Furthermore, every person identified in a whistle-blowing case, can give instructions regarding the storage, deletion and disclosure of their personal data after their death. To exercise these rights, persons identified in a whistle-blowing case can send their request by email to the following address: delegue-protection-donnees@highco.com mentioning their name, address and telephone number at which they may be contacted.

9. General information for users of the whistle-blowing system

- This procedure is available on the HighCo website https:/www.highco.com and the HighCo Group's intranet https://highco.sharepoint.com/, section Tools / Anti-corruption and charter
- This procedure is given to all employees of the HighCo Group.
- This procedure is appended to the Group's internal rules.

APPENDIX OF COMPETENT AUTHORITIES

1. Public procurement contracts:
    - French Anti-Corruption Agency (AFA), for breaches of ethics;
    - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF), for anti-competitive practices;
    - Autorité de la Concurrence, for anti-competitive practices;

2. Financial services, products and markets and prevention of money laundering and the financing of terrorism:
    - Autorité des Marchés Financiers (AMF), for investment services and market infrastructure providers;
    - French Prudential Supervision and Resolution Authority (ACPR), for credit institutions and insurance organisations;

3. Product safety and compliance:
    - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF);
    - Service Central des Armes et Explosifs (SCAE);

4. Transport Safety:
    - Direction Générale de l'Aviation Civile (DGAC), for air transport safety;
    - Bureau d'Enquêtes sur les Accidents de Transport Terrestre (BEA-TT), for the safety of overland transport (road and rail);
    - Direction Générale Des Affaires Maritimes, de la Pêche et de l'Aquaculture (DGAMPA), for the safety of maritime transport;

5. Environmental protection:
    - Inspection Générale de l'Environnement et du Développement Durable (IGEDD);

6. Radiation protection and nuclear safety:
    - Nuclear Safety Authority (ASN);

7. Food safety:
    - Conseil Général de l'Alimentation, de l'Agriculture et des Espaces Ruraux (CGAAER);
    - Agence Nationale Chargée de la Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (ANSES);

8. Public health:
    - Agence Nationale Chargée de la Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (ANSES);
    - Santé Publique France, SpF (French Public Health Agency);
    - Haute Autorité de Santé (HAS);
    - Biomedicine Agency;
    - Etablissement Français du Sang (EFS);
    - Comité d'Indemnisation des Victimes des Essais Nucléaires (CIVEN);
    - Inspection Générale des Affaires Sociales (IGAS);
    - National Institute of Health and Medical Research (INSERM);
    - Conseil National de l'Ordre des Médecins, for the exercise of the profession of physician;

- Conseil National de l'Ordre des Masseurs-Kinésithérapeutes, for the exercise of the profession of physiotherapist;
- Conseil National de l'Ordre des Sages-femmes, for the exercise of the profession of midwife;
- Conseil National de l'Ordre des Pharmaciens, for the exercise of the profession of pharmacist;
- Conseil National de l'Ordre des Infirmiers, for the exercise of the profession of nurse;
- Conseil National de l'Ordre des Chirurgiens-Dentistes, for the exercise of the profession of dental surgeon;
- Conseil National de l'Ordre des Pédicures-Podologues, for the exercise of the profession of pedicurist-podiatrist;
- Conseil National de l'Ordre des Vétérinaires, for the exercise of the profession of veterinary surgeon;

9. Consumer protection:
    - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF);

10. Protection of privacy and personal data, security of networks and information systems:
    - French Data Protection Authority (CNIL);
    - French Cybersecurity Agency (ANSSI);

11. Breaches affecting the financial interests of the European Union:
    - French Anti-Corruption Agency (AFA), for breaches of ethics;
    - Direction Générale des Finances Publiques (DGFIP), for value added tax fraud;
    - Direction Générale des Douanes et Droits Indirects (DGDDI), for fraud with respect to customs duties, anti-dumping duties and similar;

12. Internal market violations:
    - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF), for anti-competitive practices;
    - Autorité de la Concurrence, for anti-competitive practices and State aid;
    - Direction Générale des Finances Publiques (DGFIP), for corporate tax fraud;

13. Activities conducted by the Ministry of Defence:
    - Contrôle Général des Armées (CGA);
    - Collège des Inspecteurs Généraux des Armées;

14. Public statistics:
    - Autorité de la Statistique Publique (ASP);

15. Agriculture:
    - Conseil Général de l'Alimentation, de l'Agriculture et des Espaces Ruraux (CGAAER);

16. First, second and third level education:
    - Ombudsman for first, second and third level education;

17. Individual and collective labour relations, working conditions:
    - Direction Générale du Travail (DGT);

18. Employment and vocational education:
    - Délégation Générale à l'Emploi et à la Formation Professionnelle (DGEFP);

19. Culture:
    - Conseil National de l'Ordre des Architectes, for the exercise of the profession of architect;
    - French Auction Market Authority, for public auctions;

20. Rights and freedoms in relations with State administrations, local authorities, public institutions and bodies entrusted with a public service mission:
    - Défenseur des Droits (Rights Advocate);

21. Best interests and rights of the child:
    - Défenseur des Droits (Rights Advocate);

22. Discrimination:
    - Défenseur des Droits (Rights Advocate);

23. Ethics of persons carrying out security activities:
    - Défenseur des Droits (Rights Advocate).

Direction Juridique HighCo : contact-jurid@highco.fr
365 avenue Archimède – 13799 Aix-en-Provence Cedex 3