HIGHCO GROUP'S WHISTLE BLOWING SYSTEM IN BELGIUM AND SPAIN

HighCo

Preamble

In accordance with the Act of 9 December 2016 known as the "Sapin" Act, the HighCo Group adopted and then circulated in January 2018 an Anti-Corruption Code of Conduct which was updated in 2023 as well as an internal whistle-blowing system *"intended to enable employees to report conduct or situations"* contrary to this Code.

This system applies exclusively to employees of HighCo subsidiaries in Belgium (HighCo Data Benelux and Publi Info) and Spain (HighCo Spain), where such these entities employ less than fifty employees.

It is intended to enable them to make confidential reports, anonymously if they wish, concerning acts of corruption or influence peddling and other situations contrary to the HighCo Anti-Corruption Code of Conduct https://www.highco.com/investisseurs/anticorruption-conformite/.

Through this whistle-blowing system, employees of HighCo's Belgian and Spanish subsidiaries also have the possibility of reporting serious breaches of the Law as defined below.

This system is available on the HighCo website at: https://www.highco.com/investisseurs/anticorruption-conformite/ and on HighConnect[1].

In order to process the reports submitted under this system, the HighCo group has set up an Ethics Committee composed of three members, who perform the functions of Chief Human Resources Officer, Chief Legal Officer and Chief Financial and CSR Officer respectively.

[1] Corporate social network available only in Belgium.

VERSION	DATE	MODIFICATION
V1	2018	Initial version
V2	2021	Update
V3	2023	Update

TABLE OF CONTENTS

1. Who can be a whistle blower?

Any employee, including occasional employees, of HighCo Data Benelux, Publi Info and HighCo Spain, exclusively.

2. What can be reported?

Reports submitted under the whistle-blowing system must concern one or more of the following:

- Acts of corruption or influence peddling,
- Situations contrary to the HighCo Anti-Corruption Code of Conduct,
- Crimes,
- Acts of violence and racism,
- Tax fraud,
- Social fraud[2],
- Money laundering and terrorist financing,
- Breach of legal rules on consumer protection and product safety.

In particular, facts and information in the following areas may not feature in a whistle-blowing report:

- National security, except for reports of breaches of public procurement rules;
- Defence and security;
- Classified information;
- Information covered by medical secrecy and information that lawyers receive from their clients or obtain about their clients, in the performance of their duties;
- Information covered by the secrecy of judicial deliberations and lawyer-client privilege.

3. What are the prerequisites to submit a report?

To be able to submit a report, all the following conditions must be met:

1. The whistle-blower must be a natural person;
2. The whistle-blower must have become personally aware of the facts and not simply report facts observed by someone else;
3. The whistle-blower must have obtained the information in a professional context;
4. 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;
5. The whistle-blower must act in good faith: the whistle-blower must be convinced that the elements they report are true;
6. The report must concern one or more of the facts mentioned in paragraph 2 above;
7. The whistle-blower must only submit a report concerning HighCo and its subsidiaries.

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.

[2] Fraud with respect to social security contributions and benefits.

4. What protection do whistle-blowers have?

When the report meets the conditions set out in paragraph 3, the whistle-blower benefits from protection against retaliation provided by the company.

No whistle-blower who reports an event on reasonable grounds may be subject to retaliation, (for example, sanctions or any discriminatory measures), for submitting a report to the whistle-blower system described below.

The HighCo Group prohibits and punishes all forms of retaliation against those who, in good faith, report an offence. If you report a problem in good faith, and it turns out that you were sincerely mistaken, you will not be punished.

5. What other 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 European General Data Protection Regulation (GDPR).

6. How to submit the report and to whom?

You must send your report via 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 third party with the task of collecting the reports and examining their admissibility. 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 its Code of Ethics and paragraph 7 below.

The information to be communicated is as follows:

1. Your surname, first name, position and place of work; you may choose to remain anonymous;

2. The facts that you wish to communicate **in a manner sufficiently objective and precise** to enable the alleged facts to be checked. You must provide all elements, information and documents in support of your report;

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.

You can also, if you wish, make your report directly to the HighCo Group Ethics Committee via the following dedicated email address: comite-ethique@notification-highco.com.

7. How is the report 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.
- If the 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.
- If it deems the allegations to be founded, the Ethics Committee will use the means at its disposal to remedy the situation.
- The Ethics Committee will close 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 the implementation of a whistle-blowing system,
- 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

The implementation of the Whistle-blowing System is managed by the parent company of HighCo Data Benelux, Publi Info and HighCo Spain, namely: HighCo SA (353 113 566 RCS Aix-en-Provence), 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 fact-based and 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: deleque-protection-donnees@highco.com mentioning their name, address and telephone number at which they may be contacted.

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