INTELLIGENT MARKETING SOLUTIONS

WHISTLEBLOWING AND REPORTING SYSTEM

HIGHCO GROUP

As employees have been informed, in accordance with Article 17 of French Law No. 2016-1691 of 9 December 2016, known as Sapin II, HighCo SA has adopted an Anti-Corruption Code of Conduct applicable to HighCo SA and its subsidiaries located in France and abroad (hereafter referred to as the "**Group**").

The Code, which forms part of the internal regulations of the French companies, is available at www.highco.com and on the corporate social network https:/highconnect.highco.com/ in the "Human Resources" section under “agreements, internal regulation, charters and whistleblowing and reporting system”; it can also be requested from the Group's HR and Legal departments.

Alongside the Anti-Corruption Code of Conduct, Sapin II also requires an internal anti-corruption whistleblowing system ("Specific anti-corruption system") to be put in place, together with a broader system for protecting whistleblowers and receiving their reports ("General system").

For the sake of simplicity and consistency, the Group has decided to set up a **single** whistleblowing and reporting system (hereafter referred to as the "**System**"), covered by this procedure and available for consultation on the corporate social network https:/highconnect.highco.com/.

It must be stated that as part of setting up the System within the Group, the Group guarantees that it complies with French regulatory requirements and more particularly with Law No. 78-17 of 6 January 1978 relating to data protection, together with the recommendations and decisions of the CNIL (French Data Protection Authority), and more particularly its Ruling No. 2017-191 of 22 June 2017 relating to the single authorisation regarding automated processing of personal data carried out in the context of whistleblowing systems (hereafter referred to as "AU-004").

1. *Who can use the System?*

The System set up by the Group is open to:

- **all employees of** the Group;
- **external workers**, namely private individuals working on a freelance or temporary basis, and **casual workers**, namely interns;

hereafter referred to collectively as the "**Employees**".

Only private individuals can be whistleblowers; this excludes **legal entities (companies, associations or trade unions in particular).**

Use of the System is optional.

No penalty can be incurred for failure to use the System.

2. *What is the System for?*

Employees can use the System to:

1/ Disclose or report:

- A crime or offence;
- a clear, serious infringement of:
    - any international commitment duly ratified or approved by France,
    - any unilateral act by an international organisation carried out on the basis of such a commitment,
    - laws or regulations;
- a serious threat or harm to public interest.

2/ Report the existence of conduct or situations that contravene the Anti-Corruption Code of Conduct, **where these are likely to involve incidents of corruption or influence peddling.**

Reporting cannot however relate to conduct or situations covered by national defence secrecy, medical privilege and legal professional privilege.

3. What conditions are required for reporting?

Any employee wishing to make a report (hereafter referred to as the "**whistleblower**" must:

- **identify himself/herself, as anonymous reporting is not permitted***;*
- act **disinterestedly** and in **good faith** (*a person making allegations that he/she knows to be false cannot be considered to be acting "in good faith")*;
- not seek to cause **harm**;
- not **profit** from whistleblowing;
- only report **serious events** or **breaches of the Anti-Corruption Code of Conduct likely to involve incidents of corruption or influence peddling**;
- have **personal knowledge** of the facts and not, for example, be passing on mere rumours.

It is essential that these conditions are met.
In this case, the whistleblower's status is acknowledged and he/she will enjoy the specific protection described in point 6 below.

Any person abusing the System will be liable for penalties.

4. Who should the report be made to and how?

If an Employee wishes to make a report, he/she is invited to contact and identify himself/herself to the Receiver appointed by the Group, namely Mr **Jean-François Baisnée, Legal Director** (hereafter referred to as the "**Receiver").**

If he is unavailable, the Deputy Receiver, Mrs Marie Viboud, Lawyer, should be contacted.

The whistleblower makes his/her report using a form appended to this procedure, which he/she sends to the Receiver by email at the following address:

alerte@notification-highco.com

This is a confidential external email address that does not pass through the Group's IT system and is guaranteed to be confidential.

As part of the reporting process, the whistleblower can communicate with the Receiver by telephone on the following number: +33 (0)4 42 24 85 62.

In his/her report, the whistleblower must provide the Receiver with all the facts, information or documents that support the report and provide proof of the allegations.

If an Employee wishes to ask questions or receive advice regarding the Whistleblowing System and/or rules without making a Report, he/she is invited to contact the Legal Director on the aforementioned number.

5. What happens after a report is made?

Once the Receiver has received the report, he/she informs the whistleblower electronically:

- that the report has been received, by sending a receipt acknowledgement;
- of the reasonable foreseeable period required to examine the admissibility of the report and the procedures by which he/she will be informed of the action taken following the report.

The Receiver who has received the report verifies whether the report meets the aforementioned admissibility conditions (position of the whistleblower, report within the scope of the System, lack of anonymity, etc.).

If so, the Receiver sends the report file to an internal **Ethics Committee**, consisting of the HighCo Human Resources Manager, the HighCo Finance Director and the Receiver.

The Ethics Committee is responsible for examining the report file, investigating and deciding on the action to be taken.

This decision is taken within a reasonable period that may vary according to the information in the report, the complexity of the case and the progress of any investigations under way.

When performing its duties, the Ethics Committee will ensure:

- The confidentiality of all the data and information received and used during its investigation, unless the provision of said information is required by the Law;

- An exhaustive analysis of any data, information or document on which it will base its action;

The Receiver will inform the whistleblower of the Ethics Committee's reasoned decision regarding the action taken as a result of his/her report, whatever this might be.

If the Receiver does not verify the admissibility of the report within a reasonable period, indicated to the whistleblower (see above), the whistleblower may contact the judicial authority, the administrative authority (for example, the French Anti-Corruption Agency for incidents of corruption) or other professional bodies.

If the report has not been verified within a period of three months by the aforementioned bodies (judicial authority, administrative authority or other professional bodies), the whistleblower may make the report public.

As an exception, in the event of **serious, imminent danger** or if there is a **risk of irreversible damage**, the whistleblower may send his/her report directly to the judicial authority, administrative authority or other professional bodies and make it public without using the System.

These procedures must be followed for the whistleblower to enjoy the protection granted to whistleblowers.

6. What guarantees are Employees afforded?

➢ *The guarantees afforded to the whistleblower*

- No penalties

The whistleblower cannot be dismissed, penalised or discriminated against in any way for having reported the facts in accordance with this procedure, even if the facts are later found to be incorrect or do not result in any action.
Conversely, any proven abuse of the System could render the whistleblower subject to disciplinary measures and, if applicable, legal proceedings.

- Confidentiality of the whistleblower's identity

While the report is being processed, the Group will ensure that the whistleblower's identity is kept strictly confidential.

Any information that might identify the whistleblower cannot therefore be disclosed without his/her consent, except to the judicial authority.

Any person who has knowledge of the reports made under the System is bound by strict confidentiality regarding all such information, particularly as concerns the whistleblower's identity. The Receiver and the other members of the Ethics Committee have signed a specific confidentiality undertaking.

➢ *The guarantees offered to the person incriminated by a whistleblowing report*

- Information given to the person incriminated by a whistleblowing report

Any Group Employee about whom a report is made is presumed innocent until the allegations made against him/her have been proven.

The Employee about whom a report is made must be informed of the facts of which he/she is accused so that he/she may exert his/her rights, including the right to a fair hearing and compliance with the adversarial principle, as soon as the information about him/her is electronically recorded, to enable him/her to object, for legitimate reasons, to the processing of said information, where applicable.

This information, delivered securely, shall specify the name of the person managing the system, the allegations against the person about whom the report has been made and the procedure for exercising his/her right to access, correct and object to the processing of his/her personal data.

However, if it has reliable and materially verifiable information, the Ethics Committee responsible for processing the report may decide to take precautionary measures, particularly to prevent the destruction of evidence relating to the report, before informing the person incriminated by the report.

- Confidentiality of the identity of the person incriminated by the report

The identity of the person incriminated by a whistleblowing report is kept strictly confidential.
Any information that might identify the person incriminated by a whistleblowing report cannot therefore be disclosed, except to the judicial authority, until the report has been proven to be well-founded.

7. What provisions are made regarding personal data?

➢ Collection of personal data

Because setting up the System involves the collection and processing of personal data, it is subject to a **CNIL** compliance commitment in accordance with single authorisation no. AU-004.

The System is managed by HighCo SA in France, (Aix-en-Provence Register of Trade and Companies, no. 353 113 566) as the body responsible for processing.

For whistleblowing cases, only the following data categories can be recorded:

- The identity, position and contact details of the whistleblower;
- 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 reported events;
- The information collected during verification of the reported events;
- The report on the verification operations;
- The action taken following the report.

The information collected is strictly limited to the scope of the System as set out in point 2 of this procedure.

➢ *Retention period of personal data*

Data relating to a whistleblowing report deemed by the Receiver to fall outside the scope of the System will be destroyed or filed without delay, following anonymisation.

If the whistleblowing report is not followed by disciplinary or legal proceedings after investigation, the data relating to the report will be destroyed or filed, following anonymisation, by the Receiver and the Ethics Committee, within a period of two months following the completion of all the verification operations, as follows:

- Deletion of all emails relating to the terminated report;
- Destruction of all written documents relating to the terminated report.

The whistleblower and the persons incriminated will be informed of such termination.

When disciplinary or legal proceedings are brought against the person incriminated or the whistleblower in the case of an unfounded report, the data relating to the whistleblowing report is retained by the Receiver and the Ethics Committee until the end of the proceedings.

➢ *Respect for the right to access and correct personal data*

The Group guarantees to any person identified under the System the right to access his/her data and, if it is incorrect, incomplete, ambiguous or out-of-date, to request the correction or deletion thereof.

More particularly, every Employee of the Group has the right to correct, complete, update, lock or delete any of his/her personal data that is incorrect, incomplete, ambiguous or out-of-date or if the collection, use, communication or retention thereof is prohibited.

Every Employee also has the right to access, consult and object to the processing of his/her personal data for legitimate reasons.
Furthermore, every Employee may set out instructions regarding the retention, deletion and communication of his/her personal data after his death.

To exercise these rights, the Employee must send a written request by email to the following address: *delegue-protection-donnees@highco.com*, stating his/her name, address and the telephone number on which he/she can be contacted during office hours, and attaching a copy of both sides of his/her identity card or passport.

****

INTELLIGENT MARKETING SOLUTIONS

APPENDIX: FORM FOR SUBMITTING A WHISTLEBLOWING REPORT

[Note : tous les champs sont obligatoires, sauf mention contraire sur le formulaire.]

[Note: all fields are mandatory unless otherwise stated on the form.]

1. Contact details of the whistleblower:

Surname:

_____

First name:

_____

Position:

_____

e-mail adress:

_____

Téléphone number [optionnal] :

_____

2. Contact details of the person incriminated by the report:

Surname: _____ First name: _____ Position: _____ e-mail adress: _____ Téléphone number [optionnal]: _____	Surname: _____ First name: _____ Position: _____ e-mail adress: _____ Téléphone number [optionnal]: _____
Surname: _____ First name: _____ Position: _____ e-mail adress: _____ Téléphone number [optionnal]: _____	Surname: _____ First name: _____ Position: _____ e-mail adress: _____ Téléphone number [optionnal] : _____

INTELLIGENT MARKETING SOLUTIONS

1. Information about the whistleblowing report

[Note: Unless this information is vital for a clear understanding of the subject matter of the report, please do not give any sensitive information (sex life, political and religious opinions, health issues, union membership, etc.) about any private individual].

Objective description of the facts, giving the alleged reasons for the whistleblowing report:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

The information collected on this form gives rise to automated data processing managed by HighCo SA the purpose of which is to report and process whistleblowing within the Group Companies in accordance with Articles 8 and 17 of the Sapin II French Law.

Furthermore, the Employee declares, as the whistleblower, that this communication is made disinterestedly and in good faith, save for unintended errors or omissions.

He/she agrees and acknowledges that any wrongful accusation could render him/her subject to disciplinary measures or legal proceedings, where applicable.

Finally, the Employee has the right to correct, complete, update, lock or delete any of his/her personal data that is incorrect, incomplete, ambiguous or out-of-date or if the collection, use, communication or retention thereof is prohibited.

He/she also has the right to access, consult and object to the processing of his/her personal data for legitimate reasons.

Furthermore, the Employee may set out instructions regarding the retention, deletion and communication of his/her personal data after his death.

To exercise these rights, the Employee must send an email at the following address delegue-protection-donnees@highco.com, stating his/her name, address and the telephone number on which he/she can be contacted during office hours, and attaching a copy of both sides of his/her identity card or passport.