INDIGO GROUP ALERT SYSTEM PROCEDURE

INDIGO Group - June 2024 - France

INDIGO GROUP ALERT SYSTEM PROCEDURE

Message from the Chairman

INDIGO is committed to high standards of business ethics and regulatory compliance. In particular, since 2019, we have set up a whistleblowing system enabling our employees to report facts that are reprehensible from the point of view of the law or carry a risk for the general interest.

Today, we are adapting our internal procedures to enable each and every one of you, as well as our external stakeholders, to report any breach of the texts that govern us, including our internal regulations and our code of good conduct. By integrating the fields related to the duty of vigilance, i.e. human rights and fundamental freedoms, personal health and safety, as well as environmental damage resulting from the Group's activities, our procedure bears the mark of the voluntarism and seriousness of our commitment.

The compliance and integrity of our operations are at the heart of our reputation and the trust of our stakeholders. Protecting the interests of the Group, its employees, customers and partners concerns us all.

We therefore encourage you to use this confidential, secure, rigorous and impartial procedure, which will be extended by measures appropriate to the results of the resulting investigations.

We hope that this educational guide, which I hope will be distributed as widely as possible, will be a useful and useful tool for you, in the service of our collective commitment.

Sébastien FRAISSE

1. General framework

[1]The INDIGO Group's compliance policy meets both the international commitments made through its adherence to the Ten Principles of the UN Global Compact and the principles and obligations arising from the amended Sapin II law and its implementing decree.[2]

Committed to ensuring that every employee has access to a whistleblower hotline, and benefits from the protection afforded by whistleblower status (guaranteed protection against all forms of reprisal), the Group makes this procedure and the associated tools - an integral part of the Group's compliance program - available to all its subsidiaries, in Europe and worldwide.

Subsidiaries may adapt this procedure where local legal requirements do not accord with the present one, while endeavoring to apply it as closely as possible to its spirit.

The alert system includes :

- Provisions on the protection of whistleblowers (articles 6 to 16 of the Act) and on anti-corruption measures (article 17 of the Act)
- Common law measures for the protection of individuals (in particular provisions concerning sexual and moral harassment and all forms of discrimination)
- Alerts concerning serious violations of human rights and fundamental freedoms, human health and safety, and the environment

The internal whistleblowing system thus makes it possible to report facts falling within its scope, and to ensure that the reports received are handled effectively and confidentially.

It is based on the principles of good faith and respect for the rights of individuals and the defense.

this policy covers the collection and processing of alerts, and more specifically their :

- Show,
- Reception,
- Analysis of admissibility,
- Fence

The investigation procedure followed by those in charge of handling alerts is the subject of a separate document, "Internal Investigation Procedure", and is therefore not covered by this policy.

[1] https://pactemondial.org/

[2] Law n°2016-1691 of December 9, 2016 amended by law n°2022-401 of March 21, 2022 and decree n°2022-1284 of October 3, 2022

2. Terms and conditions

2.1. Which alert to report?

Facts that can be reported include :

- Conduct or situation contrary to the Indigo Group Code of Conduct,
- A felony or misdemeanor,
- A threat or harm to the general interest,
- Violation or attempted concealment of a violation of an international commitment duly ratified or approved by France or any other country whose legislation applies to the Group,
- Violation or attempted concealment of a violation of a unilateral act of an international organization taken on the basis of such a commitment, of European Union law, or of a law or regulation.
- Serious harm to human rights, human health and safety, or the environment. This infringement must result from the Group's activity or that of its subcontractors or first-tier suppliers in the context of the contractual relationship with the Group.

For example, alerts may concern the following issues: corruption, conflicts of interest, anti-competitive practices, discrimination, harassment, suspected or actual fraud.

Only facts that are unlawful or detrimental to the public interest are therefore eligible for reporting.

Thus, for all reports that do not fall within the scope of the alert procedure (normal commercial complaints, simple internal malfunctions, dissatisfaction linked to the relationship with the Indigo Group, including dissatisfaction on the part of employees with regard to their working relationship, except in the case of breaches of regulations, IT alerts, etc.), it is advisable to use the dedicated channels or the classic hierarchical route.

2.2. Who can issue an alert?

This policy applies to all internal, external or occasional employees of the Indigo Group in France (the "Employees"):

- Staff members (employees on fixed-term or permanent contracts, apprentices, trainees), as well as former employees and job applicants when the information they possess was obtained in the context of a previous employment relationship or job application.

as well as to the Stakeholders (the "Stakeholders"):

- Shareholders, associates, holders of voting rights at the general meeting of a Group entity, members of administrative, management or supervisory bodies, etc.
- External or occasional collaborators (agents, consultants, auditors, etc.)
- Group contractors (customers, suppliers, service providers, employees of subcontractors, temporary staff)
- External stakeholders (trade unions, NGOs, etc.) for breaches related to the duty of vigilance

2.3. Anonymity - Obligation of confidentiality

As a general rule, and subject to locally applicable regulations, whistle-blowing may be carried out anonymously. However, the Group encourages whistle-blowers to reveal their identity so that the alert can be handled more effectively**. In any event, the identity of the whistle-blower will be protected and treated as strictly confidential**.

Whistleblowers are invited to provide facts, information and documents to support their report (details of facts, people involved, places and dates of events).

The information and documents transmitted must be factual and directly related to the subject of the alert. They must not fall within the scope of national defense secrecy, medical secrecy, the secrecy of judicial deliberations, the secrecy of investigations or judicial inquiries, or the professional secrecy of lawyers.

Reports must be formulated in an objective, neutral and non-discriminatory manner.

2.4. How to launch an alert

Several channels are available for issuing a warning and, subject to its admissibility, enabling you to benefit from the protective status associated with whistleblower status:

- Dedicated platform: alerts can be made using the web tool provided (by service provider Euronext Group) at **https://group-indigo.integrity.complylog.com/. The** platform enables alerts, whether anonymous or not, to be received confidentially, and secure exchanges with the whistle-blower.

- Telephone line: alerts can also be made orally by the whistle-blower by telephoning a call center (managed by the service provider Isope) free of charge on the following European toll-free number: **00 800 180 620 19**. Oral alerts are transcribed in writing by the call center to the dedicated platform, in order to preserve confidentiality.

- By post: in this case, it is advisable to send the letter by registered mail with acknowledgement of receipt, in order to ensure secure delivery and enable the date of notification to be established with certainty. The letter should be addressed to Group headquarters, for the attention of the **Compliance Manager**.

The whistleblower may also request a videoconference or a face-to-face meeting. This videoconference or physical meeting will be organized no later than 20 working days after receipt of this request.

With the whistleblower's consent, alerts collected in this way will be transcribed into the platform to guarantee their confidentiality.

Whistleblowers can check, correct and approve the transcript of their alert.

Use of this warning system is optional: employees may report harassment to their superiors, Human Resources managers, harassment advisors or employee representatives.

Whistleblowers may also submit their reports to the judicial authority, the administrative authority, the Human Rights Ombudsman or the relevant professional bodies, the list of which is set out in Decree no. 2022-1284 of October 3, 2022.

[3]In the event of serious and imminent danger, or where there is a risk of irreversible damage , or where there is no response from the above-mentioned authorities within 3 months, the author of the alert is also authorized to make it public.

2.5. Conditions for the admissibility of a warning to benefit from legal protection

The alert is admissible when :

- It comes from a natural person referred to in paragraph 2.2 "*Who can issue an alert*".
- It is issued for one of the **reasons** set out in the present procedure (unlawful acts or acts detrimental to the public interest),
- The issuer acts **without direct financial consideration**
- It relates to **facts of** which the issuer has direct and personal knowledge
  On the other hand, the condition of personal knowledge of the facts is not required when the information was obtained in the course of the whistleblower's professional activity, in particular when the facts were reported to him by a competent third party.

[3] As these conditions are very restrictive, it is advisable to contact the Défenseur des droits before making a report public.

- The issuer acts in **good faith** (he must have reasonable and legitimate grounds for believing that the facts reported are true).
  Improper use of the alert system may result in disciplinary action or legal proceedings being taken against the perpetrator.
  Abusive and in bad faith is considered a denunciation of facts that the author knows to be false, or a denunciation made with the intention of causing harm, or in the hope of obtaining undue consideration, or knowingly conveying vexatious or defamatory allegations against a third party.
  On the other hand, the use of the whistleblowing system in good faith, even if the facts are subsequently proven to be inaccurate or do not give rise to any follow-up action, will not lead to disciplinary action being taken against the whistleblower, the facilitators or the persons in contact with the whistleblower.

Use of the warning system is a right freely exercised by the persons concerned, and its use remains optional. Consequently, failure to use the alert system cannot give rise to sanctions.

3. Alert processing

3.1. Receipt of alert and admissibility analysis

When an alert is made, an **acknowledgement of receipt** will be sent to the whistleblower within seven (7) working days of receipt of the alert. This acknowledgement does not constitute acceptance of the alert.

Each alert is first examined, on a confidential basis, to determine whether it **meets the conditions of admissibility** set out in paragraph 2.5 "Conditions of admissibility", and whether **there are sufficiently detailed factual elements to allow it to be processed**.

If the alert is inadmissible, its author will be informed of the reasons for its inadmissibility and of its closure. If necessary, he/she will be referred to the appropriate channel.

If the report is admissible, an internal investigation will be launched, respecting the principles of confidentiality and diligence.

3.2. Internal survey process[4]

When an alert is deemed admissible, the person who is the subject of the alert is informed of the nature of the alert concerning him or her within a reasonable period of time not exceeding one month following the issue of an alert.

[4] The investigation procedure is the subject of a separate document, "Internal Investigation Procedure", and is therefore not covered by this policy.

This information may be deferred if it is likely to seriously compromise the investigation. This is particularly the case when precautionary measures must be taken to protect people and property, and to preserve evidence.

The person who is the subject of an alert is informed of the nature of the alert and of the collection of data concerning him or her, and of the name of the person in charge of processing the alert.

The internal investigation is carried out with the aim of verifying the materiality and accuracy of the facts reported, using methods (interviews, consultation of internal documents, etc.) and participants that may vary according to the context and nature of the subject.

Alerts are handled by the General Counsel, Insurance and Compliance Manager, the Compliance Manager, the Audit and Risks Manager, the Human Resources Manager, and the Moral Harassment and Sexual Harassment Officers (the "**Alert Officers**").

Alert Referrers can contact various people (employees, customers, suppliers) to obtain the information needed to process the alert. They can also call on external experts (lawyers, accountants, analysts, etc.).

Surveys are carried out in accordance with the principles of relevance and minimization of the data collected and processed, and the confidentiality of the survey is communicated to those contacted if necessary.

In all cases, those taking part in the internal survey are informed of its confidential nature and sign a confidentiality undertaking.

Feedback is provided to the whistleblower within a maximum of three (3) months from acknowledgement of receipt of the alert or, in the absence of acknowledgement of receipt, three (3) months from the expiry of the seven (7) working day period following the alert.

It is informed of the measures taken to assess the accuracy of the allegations and, where appropriate, to remedy the matter reported, or if necessary, of the need for additional time to carry out investigations.

3.3. Closing the alert

The report is closed if the facts are not proven.

If the internal investigation establishes that the facts are true, remedial measures must be taken:

- Updating a procedure, raising awareness or training the employees concerned, reminding them of the applicable rules,
- Disciplinary measures,
- Breach of the contractual relationship with a third party when the third party is implicated,
- Legal action

The whistleblower and the persons concerned by the alert are informed in writing of the closure of the alert.

4. General principles

General

Alerts are regularly reported anonymously to General Management.

They are handled by people (Alert Referrers) who have the skills, authority and resources required to carry out their mission. The Referents carry out their mission independently and impartially, and are bound by the strictest confidentiality with regard to the elements of the investigation and the identity of the persons involved.

Employee representative bodies may be informed of the initiation, progress and conclusions of the investigation, particularly when the facts investigated fall within their prerogatives in terms of health, safety and working conditions, notably with a view to preventing psycho-social risks.

Protection of whistleblowers and facilitators

The author of an admissible report may not be subject to any disciplinary sanction, direct or indirect discriminatory retaliatory measure, or threat thereof, for having made a report in good faith.[5]

In addition, the law provides for no civil liability for whistle-blowers, and no criminal liability in the event of disclosure of confidential information, provided that such disclosure is necessary and proportionate to the protection of the interests at stake.[6]

[7][8]This protection also applies to facilitators and to people in contact with the whistleblower.

Confidentiality and managing conflicts of interest

The confidentiality of the identity of the author of the alert, of the persons concerned and of any third party mentioned in the alert, as well as the confidentiality of the information gathered, is guaranteed.

In this respect :

- Those involved in alert management are bound by a strict obligation of confidentiality, and sign a specific undertaking to this effect.
- Information identifying the whistleblower may only be disclosed with the whistleblower's consent (except to the judicial authorities).

[5] Article L.1132-3-3 of the Labor Code
[6] Article L.122-9 of the French Penal Code
[7] Any natural or legal person under private, not-for-profit law who helps the whistleblower to issue a warning.
[8] Any individual in a relationship with the whistleblower (e.g. colleague, relative, employer's subcontractor) who is at risk of retaliation.

- If the whistleblower's wish to remain anonymous or to keep his or her identity and identifying details confidential makes it impossible to carry out an investigation, the author will be informed.

All those involved in alert management undertake not to intervene in the event of a conflict of interest.

In this way, they must declare any potential, apparent or proven conflict of interest due to links that may exist with a person linked to the report (perpetrator, witness, victim, respondent).

Appendix 1

Protection of personal data

The personal data collected as part of the whistle-blowing process is processed by INDIGO PARK, the data controller, whose head office is located at "The Curve" 48-50, avenue du Général de Gaulle - 92800, Puteaux.

Purpose of processing

The purpose of the processing is, according to the content of the message :

- the collection and management of ethical alerts issued by any internal whistleblowers (including occasional employees) or external whistleblowers, relating to a breach of the Group's ethical rules and applicable anti-corruption laws and regulations (internal "anti-corruption" alert system provided for under the Sapin II law).
- the collection of whistleblower reports within the framework of the whistleblower reporting procedure (general whistleblowing system required by the Sapin II law).

Legal basis

This processing relates to compliance with legal obligations requiring the implementation of a whistleblowing system.

Categories of data processed

The categories of personal data collected directly and indirectly by INDIGO PARK are strictly necessary to verify the alleged facts and may be as follows, depending on the context:

- Identity, functions and contact details of the sender of the alert, where applicable, insofar as the author of the alert provides this data;
- Identity, functions and contact details of the persons who are the subject of the alert;
- Identity, functions and contact details of persons involved in collecting or handling the alert;
- Reported facts; Information gathered during verification of reported facts;
- Report on verification operations;
- Action taken on the alert.

Recipients of data

The personal data collected is intended exclusively for the persons authorized to receive it by virtue of their responsibilities (Compliance Officer specifically in charge of alert management) and for the persons designated by them or authorized internally, so that they can assist them in the investigation that follows receipt of the alert. Certain legal or regulatory provisions strictly restrict the communication of information (in particular, data enabling the sender of the alert or the person implicated by an alert to be identified after verification of the alert's validity), except to the judicial authorities. Should we be called upon to disclose such information, the prior written consent of the person concerned would be collected specifically.

Retention periods

The personal data collected will be kept for as long as is necessary for processing. If the alert complies with legal or regulatory obligations, but is not followed by any changes to internal rules, disciplinary proceedings or legal action, the personal data contained in the alert will be destroyed or archived after anonymization no later than two months after the end of the verification operations. When disciplinary or legal proceedings are initiated against the person(s) targeted by the alert, or against the perpetrator of an abusive alert, the personal data relating to the alert is kept by INDIGO PARK or the entities concerned until the end of the proceedings. They are then archived after anonymization or destroyed no later than two months after the end of the procedures. With the exception of cases where no action is taken on the alert, INDIGO PARK may keep the data collected in the form of intermediate archives for a minimum period in order to ensure the protection of the whistle-blower or to enable the detection of ongoing infringements. Data may be kept for a longer period, in intermediate archives, if INDIGO PARK or its entities are subject to a legal obligation (for example, to meet accounting, social or tax obligations) or if they wish to constitute evidence in the event of litigation, within the limit of the applicable prescription/forclusion period. In all other cases, the data collected are destroyed or anonymized without without delay.

Your rights

In accordance with the French Data Protection Act (Loi Informatique et Libertés) of July 6, 1978, as amended, and with European regulations on personal data, you have the right to access, modify, limit, oppose and delete your personal data. If you wish to exercise these rights or obtain information about your personal data, please contact INDIGO PARK's Data Protection Officer at dpo.fr@group-indigo.com.

You can also lodge a complaint with the Commission Nationale Informatique et Libertés.