PROCEDURE FOR REPORTING ETHICAL ALERTS

staci
FLEX-MADE LOGISTICS

January 2021 Version

Contents

1. Introduction

The STACI Group has set up a procedure for its employees, suppliers and other partners to receive alert reports that concern violations of the law or breaches of the provisions in our Code of Conduct and, more generally, any breach in terms of fundamental freedoms and human rights, the environment and occupational safety.

For this purpose, the STACI Group has appointed an Ethics Committee charged with processing and following up these reports.

Trust is paramount, which is why our alert report procedure is based on four fundamental cornerstones:

- Protection for the person raising the alert as long as they are acting in good faith;
- The presumption of innocence towards the persons named in the report;
- The proper conduct of the parties involved in gathering and processing the report;
- Respect for confidentiality.

2. Definitions

Allegation: a real or an alleged claim of a violation by a STACI member.

Alert: an allegation is made.

Laws: all legislative measures (i.e. laws, codes, regulations, rulings, directives, guidelines, policies or any other similar measures).

Violation: violation of laws or rules outlined in STACI's Code of Conduct.

Processing: refers to the actions carried out during the Alert lifecycle (from start to finish); the verb "Process" is linked to this definition.

3. Scope

Law no. 2016-1691, also known as “Sapin II” dated 9th December 2016, relates to transparency, anti-corruption and the modernisation of economic life and its implementation decree dated 19th April 2017 (no. 2017-564) established a legal framework for whistle-blowers, who have been given a unique status replacing the prior special statuses.

Under these guidelines, the new law provides for an obligation to set up a system for collecting alert reports.

Additionally, the law pertaining to the duty of vigilance of parent companies and contractors towards their subsidiaries and subcontractors of 27th March 2017 requires us to implement mechanisms to prevent human rights abuses and environmental damage throughout their production chain via an alert reporting procedure.

The scope of the alert reporting system covers compliance with all the themes in STACI’s Code of Conduct, alongside possible serious violations of laws, regulations, the revelation of crimes or offences or serious harm or prejudice to the general interest.

4. Who can whistle-blow?

A whistle-blower is a physical person (company employee or external collaborator) who reveals or reports, **in a manner** that is **impartial** and in **good faith** facts of which he or she has **personal knowledge**, relevant to the following categories:

- a crime (e.g. aggravated theft, rape, assault) or an offence (e.g. tax fraud, forgery, corruption, misappropriation of corporate assets, breach of trust, illegal taking of interest, influence peddling, threats, sexual or moral harassment, discrimination of any kind, extortion, blackmail, swindling or illegal use of public funds);
- serious and obvious violation of an international commitment duly ratified or approved by France, a unilateral act of an international organisation made on the basis of such a commitment, the law or regulations, as well as of the company’s internal regulations and code of good conduct
- a threat or serious prejudice to the general interest. For example, serious violations of human rights, fundamental freedoms, and occupational health and safety under the Duty of Vigilance Act.

Facts, information or documents, no matter their form or medium, covered by national defence secrecy, medical secrecy or the secrecy of relations between a lawyer and his/her customer are excluded from the alert reporting system as defined in this chapter.

For a full understanding of the concept of whistle-blowing, please pay close attention to the following points:

- The notion “in a disinterested manner” excludes the recourse to satisfaction of a particular interest (remuneration, revenge, etc.) and refers to an action in the general interest.
- “Good faith” refers to the absence of malice. For example, a whistle-blower who is aware of the falsity of the facts they are reporting, will not be acting in good faith.
- “Personal knowledge” of the facts presupposes: on the one hand, there is “knowledge” and not inference or supposition of the facts and, on the other, "personal" knowledge, which excludes proxy actions.

5. What protection is there for whistle-blowers?

In accordance with the provisions set out in Articles 6 to 15 of Law 2016-1691 that govern the general status of whistle-blowers, the protection of the whistle-blower includes:

- Guaranteed confidentiality of their identity;
- Prohibiting any form of discrimination or disciplinary action;
- The ability to refer the matter to the competent courts in the event of a sanction or dismissal linked to the exercise of the right to alert;
- The presumption of good faith on the part of the whistle-blower.

The use in good faith and in an impartial manner of the ethical alert reporting system - even if the facts subsequently prove to be inaccurate or do not give rise to any action - does not expose the perpetrator to any disciplinary action or any discriminatory measure, whether direct or indirect.

Nevertheless, misuse of the reporting system may expose the perpetrator to possible disciplinary action or legal proceedings. This is especially the case when it comes to slanderous accusations or fraudulent manoeuvres with the sole intention of causing harm.

6. What confidentiality exists during the process?

The procedure for collecting alert reports guarantees strict confidentiality of the author(s), the person(s) concerned and the information collected.

As such, all precautions are taken by the members of the Ethics Committee to guarantee the strict confidentiality if information likely to identify the individuals who have made a report, both in terms of collecting the report and processing it. This information particularly concerns the identity of the person at the origin of the report, their functions and their contact details.

Please remember that the identity of the whistle-blower can only be relayed to the legal authorities with their consent once the legitimacy of the alert has been established.

When recourse to third parties is necessary to process the alert, the members of the Ethics Committee must ensure that the latter are bound by a reinforced obligation of confidentiality concerning the aforementioned information.

In the same manner, all precautions should be taken by the members of the Ethics Committee to guarantee the strictest confidentiality of information likely to reveal the people involved in the report (identity, functions, contact details).

When recourse to third parties is necessary to process the alert, the members of the Ethics Committee communicate only the information that is strictly necessary and ensure that the latter are bound by a reinforced obligation of confidentiality concerning the aforementioned information.

Please remember that information likely to identify the person involved in a report cannot be disclosed, except to the legal authority, until the legitimacy of the alert has been established.

Disclosure of the information identified here as confidential is punishable by two years' imprisonment and a fine of €30,000.

7. Our procedure for reporting an alert

- 1st step: The alert should be sent to the following e-mail address:

ethics@staci.com

- 2nd step: To enable it to be processed, your report must include:
  - Your identity (which will be treated confidentially)
  - Facts, information or documents, no matter their form or medium, formulated in an objective manner that is likely to support the alert. Only the data deemed necessary to examine the merits of the report should be communicated, and the wording used to describe the nature of the facts reported should show their presumed nature;
  - If necessary, please include the elements allowing an exchange with the member(s) of the Ethics Committee. The members of the Ethics Committee may delegate part of their prerogatives to local correspondents in compliance with strict confidentiality of the procedure, for investigation purposes.

- 3rd step: The person who made the report is informed within 72 hours that it has been received by means of a written and dated acknowledgement. The acknowledgement of receipt does not, however, mean that the report is admissible.

- 4th step: Once the report has been received, it is processed by the members of the Ethics Committee and/or by the competent internal STACI Group teams, which are specially mandated for the sole purpose of verifying or processing these reports.
  Within 15 working days, the members of the Ethics Committee must inform the whistle-blower of the admissibility or inadmissibility of the alert. If the alert is admissible, they must inform the whistle-blower of the deadline for action and how he/she will be informed of the follow-up actions.

- 5th step: In the absence of the information provided for in step 4 within a reasonable time, the whistle-blower may apply to the legal authority, the administrative authority or the professional bodies.

- 6th step: Once the information transmitted has been checked, the members of the Ethics Committee will inform the author of the report by email of the follow-up actions taken due to the report via the secure platform. If the facts reported are proven correct, the members of the Ethics Committee will refer the matter to the STACI Group's management, which in turn will take appropriate measures, including disciplinary action.

- 7th step: As a last resort, if the report is not processed within 3 months it can be made public (media, etc.).

8. Data storage and information methods

Any data relating to a report that is not considered as falling within the scope of the professional alert reporting system described above will be destroyed or archived immediately after anonymisation.

Where the report does not lead to disciplinary action or legal proceedings, the data relating to the report shall be destroyed or archived, after anonymisation, within two months after completion of the checking process.

Where disciplinary action or legal proceedings are taken against the person concerned or the author of an abusive report, the data relating to the report shall be kept until the legal proceedings have been completed.

The archives shall be kept in a dedicated and secure storage space, in accordance with the GDPR policy in force at the STACI Group and applicable texts, particularly the 2017-191 resolution of the CNIL dated 22nd June 2017 (article 6), for a period not exceeding the time limits for litigation proceedings.

This procedure applies to all STACI Group staff. It is available on the intranet.

It will also be displayed on information boards at each of the STACI Group entities.