SYSTEM FOR COLLECTING ALERTS FROM WHISTLEBLOWERS

Contents

1. Definitions

Allegation: an actual or alleged assertion of a Violation by an Expleo member.

Alert: Signaling of an Allegation.

Laws: all legislative measures (i.e. law, code, regulation, rule, directive, guidelines, policy or any other measure having similar effect).

Violation: violation of the Laws or rules contained in Expleo's Code of Conduct.

Alerting: refers to any person who, in good faith and acting as a disinterested person, reports allegations of which he or she is personally aware.

Processing: refers to actions performed during the life cycle of an Alert (from its reporting to its closure); the verb "Process" is linked to this definition.

2. Scope of application

Act No. 2016-1691, also known as “Sapin II”, of 9 December 2016, regarding transparency, the fight against corruption, and economic modernisation and its implementing decree dated 19 April 2017 (No. 2017-564) established a legal framework for whistleblowers, which now has a unique status replacing special statuses that existed until then. In this context, the new law provides for an obligation to establish a mechanism for collecting alerts from whistleblowers.

Also, the Act on the vigilance duty of parent companies and general contractors toward their subsidiaries and subcontractors of 27 March 2017, requires us to set up mechanisms intended to prevent human rights violations and environmental damage throughout their production chain, via a alert reporting procedure.

The scope of the alert system covers compliance with all the themes of Expleo's Code of Conduct as well as possible serious violations of laws, regulations, the disclosure of crimes or offences or an infringement or serious prejudice to the general interest.

The Sapin II and Duty of care laws apply extraterritorially where Expleo do business. However, in the event of any breach of the rules of this policy, local law will apply.

3. Who can be a whistleblower?

A whistleblower is any person working at a company (employee or external collaborator: temp, intern, vendor) who reveals or reports, in a d isinterested manner and in good faith, facts of which they are personally aware, falling under the following categories:

- A crime or offence;
- A serious and manifest violation of an international commitment lawfully ratified or approved by the country in which we operate, of a unilateral act of an international organisation taken based on such a commitment, of the law or regulations, as well as violations of the company's Rules of Procedure.
- A threat or serious harm for the general interest. The general interest is defined as the opposition to the particular interest.

  Thus, the general interest must be understood as what is in the company's interest. For example, an employee who does not comply with Expleo's accounting procedures does not comply with the company's general interest and its above-mentioned values.

The concept of "**disinterestedly**" excludes the search for satisfaction of a particular interest and refers to an action in the general interest.

"**Good faith**" refers to the lack of intent to harm.

Personal knowledge of the facts assumes: both "knowledge" and not a deduction or assumption of the facts, and also "personal" which prevents actions by "proxy".

4. What protection is there for the whistleblower?

In accordance with the provisions of articles 6 to 15 of law 2016-1691 which govern the general status of alert launchers, the protection of the alert launcher includes:

- Guaranteed anonymity
- A prohibition against any form of discrimination or retaliation
- The possibility of petitioning the competent courts in the event of retaliation or dismissal for exercising the right to submit an alert.
- The presumption of the whistleblower's good faith

The use in good faith and in a disinterested manner of the internal alert system, even if the facts are subsequently proven inaccurate or do not result in any follow-up, does not expose the whistleblower to any direct or indirect discriminatory measures. However, abuse of the whistleblower system may expose the abuser to potential disciplinary punishment or prosecution. This is particularly the case of finger-pointing or fraudulent tactics or actions having no other intent than to harm.

5. What confidentiality does the system offer?

The alert collection system guarantees strict confidentiality for whistleblowers, for the person or persons in question, and the information collected.

Elements that may identify the person in question may not be disclosed, other than to the judicial authority, once it is established that the alert is justified.

Likewise, the elements that may identify the whistleblower may not be disclosed except to the judicial authority and with the whistleblower's consent.

The contact person (see below) and all persons required to know about the alert are subject to the same strict confidentiality obligations.

Abuse of this system may cause the whistleblower to lose their status and the associated protection.

6. Whistleblower system

6.1. Reporting step-by-step

- 1st step: The alert should preferably be sent to the confidential and secure generic platform, managed by a specialised service provider at the following address:

https://expleo.signalement.net

If necessary, the supervisor may be contacted to provide details on the operation of the internal alert system. However, other existing channels may be used.

- **2nd step**: The specialist service provider will then forward the alert to the internal referents following a possible translation. To allow for its processing, your report should include:

  - **Your identity** (which will be treated as confidential) – as an exception, and of course this is not recommended, an anonymous alert may be processed if the facts mentioned are serious enough and the alert is supported by detailed factual elements. The author of an alert who would like to remain anonymous is asked to give the internal contact persons the means to communicate with them in order to facilitate the investigation into the facts behind the alert;

  - **The facts**, information, or documents regardless of their form or format, put together objectively in a manner that supports the alert - only information needed to examine the validity of the alert must be communicated and the phrases used to describe the nature of the facts reported must show their alleged nature; and

  - Where applicable, elements enabling a discussion with the internal contact person(s).

As of 15 March 2021, the interns contact persons are Gérard BRESCON and Florence BIGOT. The contact persons may delegate a part of their powers to local correspondents, with respect for the strict confidentiality of the system, for the purposes of investigations.

- **3rd step**: The author of the alert is immediately informed, through a written, dated receipt, that their alert has been received by the internal contact person. **Confirmation of receipt however does not mean the alert is admissible**.

- **4th step**: Once the alert has been received, it is processed by the internal referents and/or by the competent internal teams of the Expleo Group, specially mandated, for the sole purpose of verifying or processing the said alerts.

  Within 15 working days, the internal referents must inform the whistleblower of the admissibility or inadmissibility of his alert. If the alert is admissible, they must inform the whistleblower of the time limit within which it will be processed and how it will be informed of the action taken.

- **5th step**: In the absence of the information provided for in Step 4 within a reasonable period of time, the whistleblower may contact the judicial authority, the administrative authority or the professional orders.

- **6th step**: Once the verification of the information transmitted has been completed, the internal referents will inform the author by email of the action taken on his report via the secure platform. If the facts reported are confirmed, the referents will refer the matter to the management of the Expleo Group, which must respond appropriately, including disciplinary measures.

- **7th step**: as a last resort, if the alert is not processed within a period of 3 months, the whistleblower may make the alert public (media, etc.)

6.2. Data retention

All data related to a alert that is considered as not falling under the scope of the professional whistleblower system described above will be destroyed or archived immediately after anonymization.

If the alert is not followed by a disciplinary or legal procedure, the data related to this alert is destroyed or archived, after anonymization, within a period of two months starting from the closure of verification operations.

When a disciplinary procedure or legal action is taken against the person in question or the author of an abusive alert, the data related to the alert is retained until the end of the legal proceeding.

With regard to archives, they will be retained in accordance with the general archiving policy applied within the Expleo group, for a period not exceeding the time for litigation proceedings.

7. Information terms

This procedure applies to all Expleo group staff. It is available on the intranet. It is also posted on the information boards in each of the branches.