PROCEDURE RELATING TO THE EVEN GROUP WHISTLEBLOWING SYSTEM

VERSION 2023

REFERENCE: V1-2023

WRITTEN AND EDITED BY THE EVEN GROUP LEGAL AND COMPLIANCE DEPARTMENT

SUMMARY

I. PREAMBLE

The purpose of this Procedure is to explain the Whistleblowing System as provided for by the regulations in force, i.e.:

SAPIN II ACT AND WASERMAN ACT	➲Act No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (hereinafter referred to as the "Sapin II Act"); ➲ Act no. 2022-401 of 21 March 2022 to improve the protection of whistleblowers (hereinafter referred to as the "Waserman Act"); ➲ Decree no. 2022-1284 of 3 October 2022 on the procedures for collecting and processing whistleblower alerts and setting the list of external authorities established by Act no. 2022-401 of 21 March 2022 to improve the protection of whistleblowers (which repealed Decree no. 2017-564 of 19 April 2017 on the procedures for collecting whistleblower alerts within legal entities governed by public or private law or State administrations).
DUTY OF CARE	➲Act 2017-399 of 27 March 2017 on the duty of care of parent companies and ordering companies.

The purpose of the Procedure is, in particular:

- To define the scope of the System and the objectives pursued;
- To set out the operating procedures for the System and the facts likely to fall within its scope;
- To present the guarantees offered by this System.

This current whistleblowing system puts an end to the previous whistleblowing system, which was accessible from the following email address alerte-code-conduite@even.fr. Therefore, notifications can no longer be sent to the aforementioned email address.

DEFINITIONS

"**Alert(s)"**: "Alert(s)" means an Alert that meets all the conditions of this Procedure. The Alert is therefore qualified as an Alert when all the conditions of the Procedure are met.

"**Author***":* "Author" means the person who submits a Report on the Platform.

"Recipient(s)*:* recipient(s)" means the person who collects and processes the Report submitted by the Author on the Platform.

"**System"**: "System" means the internal whistleblowing system used to collect and process the reports submitted by the Author on the Platform.

"**Platform**": "Platform" refers to the online whistleblowing system offered by VISPATO[1]. This Platform enables the Even Group to collect and process Reports. Use of the Platform is defined in Article VII below.

"**Procedure**": "Procedure" means this document, which describes, in particular, the terms and conditions for applying and implementing the System.

"**Report(s)"**: "Report(s)" refers to any fact and/or information reported via the Platform defined in Article VII below.

[1] https://www.vispato.com/fr/

II. SCOPE OF APPLICATION AND ACCESS TO THE PROCEDURE

The Procedure and the System apply to all employees and associates of the Even Group (including within the companies it controls, within the meaning of Article L233-1 et seq. of the French Commercial Code). For employees and associates, this system is a complement to the other existing means of reporting: through the hierarchy, to the human resources department and to staff representation bodies.

The Procedure and the System are also applicable to any third party as referred to in article V of the Procedure in the context of the exercise of duty of care.

The Even Group guarantees the dissemination of the Procedure to all and by any means ensuring sufficient publicity, in particular by notification, posting or publication and also electronically on the Even Group website accessible at the following address: https://www.even.fr/ under the heading "Alert" (at the bottom of the home page). A link to the above URL address is provided on the websites of Even Group subsidiaries.

This Procedure can also be accessed via the Even Group's internal portal via the following path: *Publications/Even Group/Library/06.Legal information/Compliance/Whistleblowing system.*

Access to this Procedure is therefore advertised both internally and externally.

III. THE SCOPE OF THE SYSTEM

a. The objectives pursued

The system has been set up by the Even Group to enable the reporting of acts and/or behaviour that may violate the integrity and/or rights of individuals, affect the Group's business or give rise to serious liability. The system implemented by the Even Group guarantees the Author of the Alert total confidentiality and the absence of repercussions when the Author is acting in good faith.

b. The areas covered by the System

The purpose of the System is to process Alerts relating to:

- A crime, an offence;
- A threat or serious harm to the public interest;
- Violation or attempted concealment of a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organisation taken on the basis of such a commitment, of European Union law, or of a law or regulation.

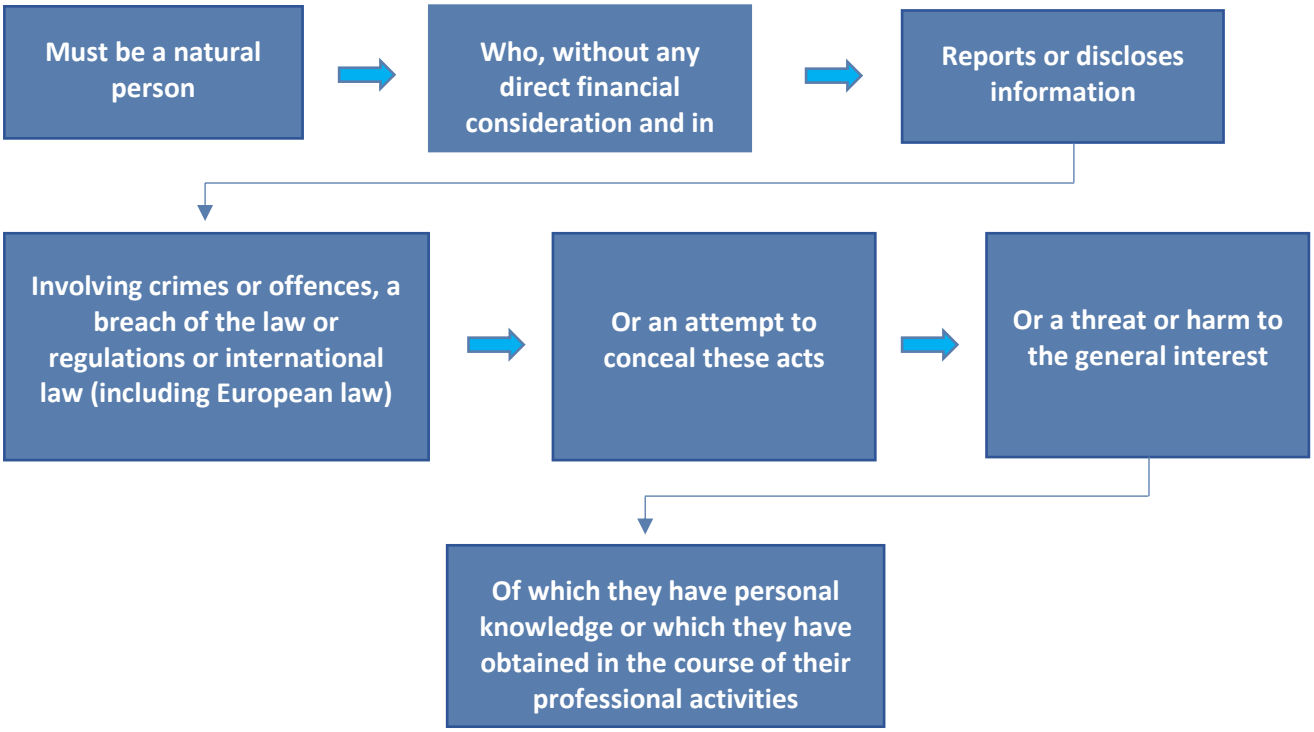
Whistleblowers can report any failure or incident relating to, but not limited to, the following areas:

- Human rights (e.g. child labour);
- Fundamental freedoms (e.g. violation of the right to strike, recognised as a fundamental freedom for employees);
- Personal health and safety (e.g. psychosocial risks such as work overload);
- Environment (e.g. pollution);
- Product safety and conformity (e.g. health risks);
- Corruption, fraud, theft, swindling, money laundering;
- Anti-competitive practices (e.g. anti-competitive agreements);
- Moral or physical harassment, discrimination, forced labour, infringement of trade union rights;
- Protection of personal data (large-scale data leakage, for example);
- International sanctions and embargoes;
- Non-compliance with the Even Group Code of Conduct.

Facts, information and documents, whatever their form or medium, the revealing or disclosure of which is prohibited by the provisions relating to **national defence confidentiality, medical confidentiality, the confidentiality of judicial deliberations, the confidentiality of judicial investigations or proceedings or the professional confidentiality of lawyers**, are excluded from the scope of the System.

IV. THE PERSON WHO MAKES A REPORT

The person who makes a Report:



The following clarifications are in order:

- The reporting person is not necessarily the whistleblower; he or she may simply be an "informant" on the breaches observed;
- The reporting person must not receive any direct financial consideration in exchange for their report;
- The person making the report may report the commission of the acts or their concealment;
- In addition to facts of which they have personal knowledge, the person making the report may also report facts, of which they have indirect knowledge in their professional capacity (via employees, shareholders, external associates, contractors, sub-contractors, etc.);
- Reports must relate to events that have occurred or are clearly likely to occur in the entity concerned.

V. WHO CAN MAKE A REPORT?

The right to issue an alert belongs to:

➲ Members of staff, to persons whose employment relationship has ended, where the information was obtained in the course of that relationship, and to persons who have applied for employment with the entity concerned, where the information was obtained in the course of that application;

➲ Shareholders and cooperative shareholders, members and holders of voting rights at the general meeting of the company concerned;

➲ Members of administrative, management or supervisory bodies;

➲ External and occasional collaborators;

➲ Co-contractors of the entity concerned, their sub-contractors or, in the case of legal persons, to the members of the administrative, management or supervisory bodies of these co-contractors and sub-contractors and to the members of their staff;

➲ Any third party, for breaches of duty of care.

Any person who obstructs the transmission of an alert in any way whatsoever is punishable by one year's imprisonment and a fine of 15,000 euros.[2]

VI. THE PERSON IN CHARGE OF THE SYSTEM

Alerts will be centralised, collected and processed for all subsidiaries and/or companies controlled by the Even group, at the Even group level.

The Head of the System is the Even Group's Human Resources Director.

Depending on the type of Report, the recipients of these Reports who are required to collect and process them will be as follows:

- Even Group Human Resources Department
- Even Group Legal and Compliance Department

Each recipient of the Report must treat it confidentially, seriously, completely and impartially.

VII. REPORTING PROCESS

a. Access to the online declaration platform

The Even Group has selected the "Vispato" secure platform to collect, process and manage all exchanges and information relating to Alerts.

The URL link to this Reporting Platform, which is accessible to all, is as follows: https://signalements-even.vispato.com/.

This Platform can also be accessed via the Even Group's internal portal via the following path: *Publications/Even Group/Library/06.Legal information/Compliance/Whistleblowing system.*

[2]Article 12-1 I. of the Sapin II Act

Access to this Platform is therefore advertised both internally and externally.

The Platform is also available by scanning the following QR Code:

This Platform is available:

- 7 days a week, 24 hours a day (excluding maintenance periods);
- Regardless of the country in which the Author is located;
- In French and English.

b. Written nature of the Report

The reports submitted on the Platform referred to in a) above must be in writing only.

c. The content of the Report

All reports must contain the following information:

- The identity, e-mail address and job title of the person submitting the Report, unless the person submitting the Report wishes to do so anonymously;
- Where applicable, if a person is the subject of a Report, the identity and position of that person;
- The subject of the Report;
- A description of the facts reported (the description of the facts must be precise and accurate. Any elements of context that may be useful in understanding the facts must be indicated;
- Any information or documents that support the Report and the seriousness of the facts reported.
- Confirmation from the Author that they are aware of this procedure before submitting their Report.

d. Collecting the Report

Following each Report filed on the aforementioned Platform, the Author will be informed in writing, via the Platform, of the receipt of his/her Report within **seven working days of receipt**.

Acknowledgement of receipt within seven working days of notification

e. Terms and conditions of access to the Platform by the Author after submitting a Report

Once the Report has been submitted, the Author will be given a URL link to view the Report and a password via the Platform. Using this link and the password (access data), a secure, encrypted dialogue box will be created so that the Author can check the progress of the case and answer any questions. It is the responsibility of the Author to regularly connect to this dialogue box. Exchanges will take place exclusively within this secure and encrypted dialogue box.

Without the access data, the Author will not be able to access the Report filed, its status and, where applicable, answer the questions asked. Consequently, access data must be kept by the Author in a secure location, who may download them.

In addition, the Authors of the Report(s) may export their Report(s) in PDF format as proof of submission of the Report(s) if required.

f. Admissibility analysis

Except in cases where the Report is anonymous, the Author must transmit, at the same time as his Report, any evidence proving that he belongs to one of the categories of persons mentioned in V above.

The recipient of the alert must check that:

- The Report falls within the scope of this Procedure (unless the Report is anonymous);
- The claims are sufficient;
- The allegations are true.

The Recipient may request any additional information from the Author.

The Recipient shall communicate information on the measures envisaged or taken to assess the accuracy of the allegations and, where applicable, to remedy the subject of the Report, as well as the reasons for such measures in writing via the Platform, to the Author, within a reasonable period of time not exceeding **three months from the acknowledgement of receipt of the Report or, in the absence of acknowledgement of receipt, three months from the expiry of a period of seven working days following the Report**.

Communication to the Author within a maximum of three months from the AR. In the absence of an AR, three months from the expiry of a period of seven days following

Reporting is anonymous

For Reports received anonymously, the consequences are as follows: the Report will be taken into account by the Recipient and will be analysed. However, if at an advanced stage of the analysis, it appears to the Report Recipient that knowledge of the person is essential in order to complete the analysis, the entity may require the Author to disclose his/her identity. In this case, the identity of the Author will only be known to the Recipient of the Report, unless there is a need for wider communication. The Author will then be informed of the persons having knowledge of his identity so that he can give his consent beforehand.

The Report is declared inadmissible after the admissibility analysis.

The Recipient will inform the Author, via the Platform, of the reasons why the Report is inadmissible (for example: the Report does not fall within the scope of the System, failure to comply with the Procedure, inaccurate or unfounded allegations or when the Report has become irrelevant). The action taken on this type of alert is as follows: the alert is closed.

The Alert is declared admissible following the admissibility analysis: processing of the Alert

When the Report is declared admissible and the allegations appear to be substantiated, the Report is classified as an Alert.

The Recipient implements the means at its disposal to remedy the subject of the Alert.

g. Alert instruction

Any person who may be the subject of the Alert must be informed, within a reasonable time and at the latest within one month from the start of the processing of the Alert by the Recipient, of the filing of an Alert concerning them by email or via the Human Resources department. They may be granted access to the Report filed on the Platform.

The person concerned by the Alert must also be informed by the Recipient of the data concerning them. In particular, they must be informed of:

- ⇨ The facts they are accused of,
- ⇨ The list of persons informed of the Alert concerning them (except the Author of the Alert),
- ⇨ The procedures for investigating and closing the Alert,
- ⇨ How to exercise their rights of access and rectification.

On the other hand, when precautionary measures are necessary, in particular to prevent the destruction of evidence relating to the Alert, the person concerned by the Alert is only informed once these measures have been taken.

The Recipient then immediately carries out an internal investigation of the Alert to verify the reality of the facts and to determine the action to be taken on the Alert.

Depending on the nature and detail of the information provided by the Author of the Alert, the Recipient may decide to carry out additional investigations, which it may entrust to internal departments (human resources, fraud, audit, etc.) or to external experts (lawyers, private investigators, etc.).

In this case, only the data required to verify and process the alert is sent to internal departments and/or external experts. They must keep the information they provide strictly confidential.

At the end of the Alert verification and processing operations (including additional investigations if any), an investigation report is sent to the Recipient by the persons contacted. This report is accompanied by the documents and information collected during these investigations.

The Recipient then decides what action to take on the Alert, with the Human Resources Department and/or Even Group General Management, where appropriate, if the seriousness of the Alert so warrants. This decision is taken on the basis of the investigation report(s) and the documents and information gathered during the investigation.

Action taken in response to the Alert may include, but is not limited to the following:

- No further action;
- Disciplinary sanctions;
- In accordance with Article 5 of the Waserman Law, the Alert is forwarded to the judicial authority.[3]

Finally, within a reasonable period of time, the Author of the Alert and the person who may be the subject of the Alert are informed by the Recipient of the action taken on the Alert.

3 In accordance with Article 5 of the Waserman Act, it is specified that *"information likely to identify the whistleblower may only be disclosed with the whistleblower's consent. It may, however, be communicated to the judicial authorities* ***if the persons responsible for collecting or processing the reports are required to report the facts to the judicial authorities [...]***".

h. *Integrity and confidentiality*[4]

The integrity and confidentiality of the information collected in the context of a Report, in particular the identity of the Author of the Report, the persons referred to in the Report and any third party mentioned in the Report, are guaranteed.

Access to information gathered in the context of a Report is prohibited to members of staff other than those authorised and provided for in Article VI of this Procedure.

Signals received by other persons or services shall be forwarded without delay to the members provided for in Article VI of this Procedure.

Information that may identify the Author may only be disclosed with the Author's consent. It may, however, be communicated to the judicial authorities if the persons responsible for collecting or processing the Reports are required to report the facts to the judicial authorities. The Author will then be informed, unless such information would compromise the legal proceedings. Written explanations are attached to this information.

Information that may identify the person implicated by an Alert may only be disclosed once it has been established that the Alert is well-founded, except for disclosure to the judicial authority.

VIII. PROTECTING THE AUTHOR: WHISTLEBLOWER

The Author of an Alert who meets the conditions defined by the present Procedure benefits from the status of whistleblower.

In this context and in accordance with the regulations in force, the whistleblower is not criminally liable (article L122-9 of the French Penal Code). The whistleblower is also not civilly liable for damage caused by his or her Whistleblowing if he or she had reasonable cause to believe, at the time he or she made the Whistleblowing Report, that it was necessary to protect the interests at stake.

In this respect, the whistleblower may not be subject to any retaliatory measures, threats or attempts to resort to such measures, in particular in the forms defined in article 10-1 of the Sapin II law (for example: suspension, lay-off, dismissal or equivalent measures, demotion or refusal of promotion, transfer of duties, change of workplace, reduction in salary, change in working hours).

The protection afforded to whistleblowers also applies to the persons defined in article 6-1 of the Sapin II law.

[4] Disclosing confidential information (obtained as part of the System) is punishable by two years' imprisonment and a fine of €30,000 in accordance with article 9.II of the Sapin II law.

IX. INTERNAL CONTROLS

Types of control	Control content	Applicable procedure
Level 1 controls	Level 1 controls will be carried out to monitor the deployment and correct application of the Procedure and will cover, in particular,: • Accessibility of the Report reception channel; • The Procedure's internal communication; • Acknowledgement of receipt; • Analysis of the admissibility of the Report; • Closing the investigation; • Sanctions and action plans in place; • Respect for confidentiality and anonymity; • Monitoring the protection measures put in place.	These controls are formalised and documented. They are carried out by the System Manager in accordance with the frequencies specified in the inspection plans.
Level 2 controls	Level 2 controls involve regular checks to ensure that level 1 controls have been carried out correctly, on the basis of representative samples of files.	Level 2 controls are carried out by the Even Group's Legal and Compliance Department and are the subject of a formalised control plan describing, in particular, the scope of the controls, the roles and responsibilities, the frequency, the sampling methods, the expected formalisation, the follow-up of anomalies and the associated action plans.
Level 3 controls	Level 3 controls will be carried out by the Even Group Audit Department.	

Any Report which reveals fraudulent behaviour or a major failure in internal control will give rise to appropriate measures and recommendations.

In the context of controls (levels 1, 2 and 3), employees carrying out internal controls (by virtue of their duties) will be able to access information transmitted in Alerts and in processing files.

The results of controls (levels 1, 2 and 3) will be reported to the Even Group's Executive Committee via the control report at least once a year.

X. WHISTLEBLOWING SYSTEM REPORTING

The Even Group Legal and Compliance Department regularly informs the Even Group Management Committee of the number of Alerts received (via the VISPATO Platform) and the action taken on the Alerts, in particular the measures implemented to remedy the Alerts received, without violating the obligations of confidentiality and anonymity.

XI. DATA RETENTION AND CONFIDENTIALITY

The data collected through the System is processed in accordance with the applicable personal data regulations and in particular with the requirements of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing the directive 95/46/CE (called "GDPR").

All necessary precautions are taken to protect the security of data when it is collected, communicated or stored.

a. Personal data collected and processed

The Even Group ensures that only relevant and necessary information with regard to the purposes of processing is collected and/or stored in the System.

This may include the following data:

- The Author's identity, duties and contact details (telephone number, e-mail address, etc.);
- Identity details, functions and contact details of persons involved in collecting and/or processing the request;
- Identity data, functions and contact details of the persons concerned by the Report and of any witnesses;
- Data on reported incidents;
- Information gathered as part of the verification of the facts reported (preliminary analysis of the Report, then, where appropriate, processing and investigation of the Alert).

The Even group may also indirectly collect personal data which would be provided by other notifiers, hierarchical superiors, persons involved and other authorised persons participating in the investigation of a question / Report.

The Even Group (data controller) uses the VISPATO Platform (service provider which processes personal data on behalf of the data controller). In this context, the Parties have signed a personal data processing agreement (in accordance with Article 28 of the GDPR) relating to the VISPATO whistleblowing system.

b. The personal data retention period

As a preliminary point, it is hereby specified that the retention periods used in this Procedure are those described in the CNIL's reference document "relative to processing of personal data intended to implement the whistleblowing system" of 6th of July 2023.

Personal data relating to a Report is kept for the time needed to receive and analyse it.

Personal data relating to an Alert considered not to fall within the scope of the System (inadmissible Alert) is destroyed immediately or made anonymous.

Personal data relating to a Report considered to fall within the scope of the System is kept in the active database until a final decision is taken on the action to be taken.

Personal data relating to an Alert considered to fall within the scope of the System (=an Alert) and giving rise to a follow-up:

- If no disciplinary or litigation proceedings are initiated against a person implicated or the Author of an abusive Alert: the data collected will be kept for a maximum period of one (1) year in the active database; for the purposes of ensuring the protection of the Alert Initiator and enabling the establishment of ongoing offences.
- If disciplinary or litigation proceedings are instituted against a respondent or the Author of an abusive Alert: the data relating to the Alert will be kept in the active database until the end of the proceedings or the limitation period for appeals against the decision.

In both cases, the data will then be stored in an intermediate archive for a period of time strictly proportionate to its processing and the protection of its authors, the persons it concerns and the third parties it mentions, taking into account the time required for any further investigations.

At the end of the above retention periods, personal data will be securely deleted from all servers or made anonymous.

c. Personal data rights

As part of the processing that the Even Group carries out on the personal data detailed above, the persons concerned have the following rights: right of access, modification, deletion, restriction and opposition. These rights may be exercised by contacting the Even Data Protection Officer (DPO) at the following email address dpo@even.fr

d. Non-personal data

Non-personal data (such as reports containing no personal data and/or that cannot be linked to a natural person) will be retained for the same periods as personal data, depending on their classification (inadmissible report, report not followed up, report falling within the scope of the System, etc.).

XII. USE OF THE SYSTEM IN GOOD FAITH

The System must be used in good faith. Therefore, the purpose of filing a Report on the Platform must not be to harm anyone, to make false accusations and/or to gain personal advantage.

Misuse of the System (for example, a Report relating to facts that the Author knows to be false) may expose the Author to disciplinary sanctions and, if necessary, legal proceedings.

XIII. EXTERNAL REPORTING

Pursuant to article 8.II of the Sapin II law, any person has the alternative option of making an external alert.

This external notification can be made to the competent external authorities, namely:

- To the competent authority among those designated by Decree no. 2022-1284 of 3 October 2022 relating to the procedures for collecting and processing alerts issued by whistleblowers and establishing the list of external authorities instituted by Law no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers. The competent external authority differs according to the area concerned by the alert.

- The Defender of Rights, who will direct the complainant to the authority or authorities best placed to deal with it;

- The judicial authorities;

- An institution, body, office or agency of the European Union competent to collect information on breaches falling within the scope of the aforementioned Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

END