



a coesia company

Whistleblowing Policy

Volpak S.A.U. (Spain)

Contents

General information	3
Part A - VOLPAK'S INTERNAL REPORTING SYSTEM	4
Part B - REPORTING	6
Part C - GUARANTEES OF VOLPAK'S INTERNAL REPORTING SYSTEM	8
Part D - PROCESSING OF PERSONAL DATA	10
Part E - NON-RETALIATION	12
Part F - EXEMPTION AND REDUCTION OF THE PENALTY	13

Volpak, S.A.U.

P.I. Can Vinyalets, 4,
08130 Sta. Perpetua Mogoda, Barcelona / Spain,
T (+34) 93 5446700, F (+34) 93 5741136.

Volpak, S.A. Sociedad Unipersonal. Inscrita en el R.M.B. Tomo 30613, Folio 171,
Hoja B-176133, Inscripción 9ª N.I.F. A-80.280.407. (VAT.ES A-80.280.407)
main@volpak.com
www.volpak.com

General information

This informative document regarding the whistleblowing policy of VOLPAK, S.A.U. (hereinafter, “Volpak” or the “company”), a Coesia group company, is written in accordance with the Coesia Code of Ethics, the Coesia Global Whistleblowing Policy and Spanish legislation.

The reporting persons can choose if to submit their report through the Coesia whistleblowing channel (at Group level) or directly at Volpak’s whistleblowing channel, as follows:

a. Group Level - Coesia

Following the Coesia Global Whistleblowing Policy, reports made through the Coesia whistleblowing channel are received by the Coesia Ethics Committee – an independent and autonomous body chaired by the President of Coesia – and by the Coesia Global Whistleblowing Management Team.

b. Local Level – Volpak

According to Volpak’s Protocol regulating its Internal Reporting System, reports posted through Volpak’s whistleblowing channel are received by its Internal Reporting System Management Committee, composed of two members from the Coesia headquarters and two local members.

A. VOLPAK'S INTERNAL REPORTING SYSTEM

In compliance with Spanish Law 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption, the Coesia Code of Ethics and the Coesia Global Whistleblowing Policy, VOLPAK hereby certifies that it has an Internal Reporting System, in which the company acts as the controller in the processing of personal data, in accordance with the current law on this matter.

In order to strengthen the culture of information and of the infrastructure of integrity of the said company, and to foster the culture of communication as a mechanism for preventing activities or omissions that might constitute criminal or serious or very serious administrative offenses, the company has appointed an Internal Reporting System Management Committee, which is made up of two members from the Coesia headquarters and two local members.

The two local members will be referred to as the “Local Contact Persons”.

To this end, in accordance with Law 2/2023, one of the Local Contact Persons has been given the job of System management and the processing of the investigation files regarding the information received through the Internal Reporting System covered by said regulation (the “Delegated System Manager”).

B. REPORTING

Anyone can submit a report. In accordance with the Coesia Global Whistleblowing Policy, Volpak extends the possibility of reporting to all individuals who, in the context of their work-related activities, become aware of a possible violation.

Once a notification is received, in accordance with the Internal Reporting System Management Committee, the Local Contact Persons will coordinate the investigation plan, if necessary. The Coesia Ethics Committee will be informed regarding the results of the investigation and the Internal Reporting System Management Committee will propose measures to such Committee for approval.

How to report:

(As mentioned, the reporting persons can choose if to submit their report at Coesia Group level or directly at Volpak via the online platform identified below.)

WRITTEN FORM

Through the reporting digital platform accessible online via:

- computer at the following link **coesia.ethicspoint.com**;
- mobile at **coesia.navexone.eu** or by scanning the **QR code**:

**ORAL FORM**

- toll-free numbers are available on the portal **coesia.ethicspoint.com** (24h – 7 days a week)

(The above channels allow anonymous reporting)

After submitting the report, the Whistleblowers will receive an access code called a 'report key' which, along with a password, can be used to check for any reply or questions on the platform.

Anonymity and Confidentiality

Whistleblowers can report:

- **Openly:** Whistleblowers provide full details of their personal contact details;
- **Anonymously:** Whistleblowers can choose to provide their contact email to the NAVEX platform, this will not be forwarded to Coesia or VOLPAK or any of its companies, but will enable the reception of notification emails when a reply or question is posted in the system or remain completely anonymous. In this case, it will be up to the Whistleblowers to use their password and 'report key' to access the system to check for feedback.

PERSONAL MEETING

On request by the whistleblower, the information may also be reported at a face-to-face meeting with the Delegated System Manager of VOLPAK within a maximum of seven days, writing at the email address: stefano.fornaro@volpak.com. Verbal reports made in a face-to-face meeting or by phone will be recorded in accordance with current regulations.

C. GUARANTEES OF VOLPAK'S INTERNAL REPORTING SYSTEM

Volpak's Internal Reporting System meets the requirements of Article 5.2 of Law 2/2023 insofar as:

- a. It allows for those to whom said Law applies to report information via various channels on the violations set forth in its Article 2.
- b. It is managed securely, ensuring that communications can be treated effectively within the company, along with the confidentiality of the identity of the whistleblower and any third party mentioned in the communication, and the action taken in its management and processing, as well as the protection of data, preventing access by unauthorized personnel
- c. It is governed by a specific policy (the Protocol on the Internal Reporting System, the use of the Internal Reporting Channel, and regulating the functions of the Internal Reporting System Management Committee) (Information Management Procedure) which establishes guarantees for the protection of whistleblowers, including:
 - Written proof of receipt within seven calendar days following receipt of the information.
 - A maximum of three months to respond to the actions of the investigation, under the terms of Article 9 of Law 2/2023, completing and diligently safekeeping an Information Logbook.
 - Possibility of remaining in contact with the whistleblower.
 - Establishing the right of the person affected to be informed of the actions or omissions being attributed to them and their right to be heard.
 - Guarantee of confidentiality when the communication is sent via reporting channels that are not those indicated or to personnel not responsible for its processing, as well as the obligation of the person receiving it to send it immediately to the System Management Committee.
 - Respect for the presumed innocence and the honor of those affected.
 - Respect for Data Protection provisions (Title VI Law 2/2023).
 - Commitment to send the information to the Public Prosecution Service immediately when the events may prove to constitute an offense.

D. PROCESSING OF PERSONAL DATA

VOLPAK shall process the personal data included in the communications received and is covered by Law 2/2023, as the controller, in order to be able to manage them and commence, where appropriate, the corresponding investigation procedure. The lawful basis for processing shall be compliance with a legal obligation arising from the Law of reference.

Where the communication contains special data, the lawful basis shall be essential public interest and other provisions set forth in Art. 9.2.2 of 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.

Furthermore, it has been indicated that this personal data may be processed and transferred by personnel authorized to do so only when this is necessary to take corrective measures in the company or for the processing of any sanctioning or criminal proceedings that may apply. The personal data shall be stored for the time required to decide on the suitability of commencing an investigation into the events reported.

On all accounts, where this decision is not made within three months, the personal data contained in the communication shall be erased, except to maintain evidence of system operations and always anonymously.

Any personal data not considered truthful shall also be erased, except where this lack of truthfulness may constitute a crime in which case the information shall be saved for the time required for the legal proceedings to be processed.

Finally, it is hereby certified that the whistleblower may at any time ask the controller for access to their personal data, for its rectification or erasure or for its restricted processing, or may object to said processing, and are also entitled to the portability of their data by sending an e-mail to privacy@volpak.com with a photocopy of their identity document attached.

In the event of disagreement with the processing of your data, you may file a claim with the Spanish Data Protection Agency, the regulatory authority on the matter, located at C/ Jorge Juan, 6 (28001) Madrid (www.aepd.es).

E. NON-RETALIATION

VOLPAK expressly undertakes not to take any action that may constitute retaliation, including threats or attempted retaliation against whistle-blowers, in accordance with Law 2/2023, and to apply measures while a file is being processed to protect those affected by a possible communication.

F. EXEMPTION AND REDUCTION OF THE PENALTY

Whenever a person who took part in the administrative offense included in the information is the one to inform of its existence by reporting the information, and whenever this is presented prior to their being notified of the start of the investigation or sanctioning procedure, the body responsible for settling the procedure by way of a reasoned decision may exempt them from fulfilling the corresponding administrative penalty provided the indications of Article 40 of the Law of reference can be accredited.

Although the Internal Reporting Channel shall preferably be used whenever possible, if the circumstances and the severity of the communications require as such and the whistleblower so decides, they may also be sent to the Independent Whistle Blower Protection Authority or to the corresponding regional authorities or bodies, to the Public Prosecution Service, or to the European Prosecution Service, as appropriate.