



WHISTLEBLOWING SYSTEM POLICY

*(update of the Whistleblowing System Policy published by VERALLIA S.A. in September 2018 –
updated on May 2022)*

Contents

1. Introduction.....	1
1.1. Objectives.....	1
1.2. Definitions.....	1
1.3. Scope.....	2
1.4. Roles and Responsibilities.....	3
2. The Alerts and the Whistleblowing System.....	4
2.1. Flowchart.....	4
2.2. What should be reported?.....	4
2.3. Who can raise an Alert?.....	5
2.4. Content and Language of Alerts.....	5
2.5. How to raise an Alert?.....	6
2.6. Management of Alerts.....	7
2.7. Investigation.....	7
2.8. Communication with the Whistleblower.....	8
3. General Principles.....	8
3.1. General.....	8
3.2. Confidentiality.....	8
3.3. Protection of personal data.....	9
3.3.1. Personal Data.....	9
3.3.2. Retention of personal data.....	10
3.3.3. Transfer of the Data outside of the European Union.....	10
3.3.4. Rights of individuals.....	11
4. Reporting to the Compliance Committee.....	11
5. Contacts.....	11

1. Introduction

1.1. Objectives

In accordance with Verallia's values – **respect for people, laws and the environment** – and as a part of the implementation of an approach in line with its *Code of Conduct and its Anti-Corruption and Anti-Trading in Influence Policy*, Verallia has implemented a Whistleblowing System complying with Article 8, paragraph III and Article 17 of the law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of the Economy ("Loi Sapin 2") and with the decree No. 2017--564 of April 19, 2017 on the procedures to receive Alerts from Whistleblowers within legal entities governed by public or private law or government administrations.

The Whistleblowing System enables every Verallia Collaborator and Partner to report in good faith actions that potentially contradict the legal obligations, or the Code of Conduct, or the Group's Anti-Corruption and Anti-Trading in Influence Policy, under the conditions defined below.

Verallia expects its Collaborators as well as its Partners to act in accordance with the laws, codes, professional standards, as well as applicable directives, policies and procedures.

This Policy constitutes an integral part of Verallia's Compliance Program.

1.2. Definitions

- **Professional Alert/Alert:** each report transmitted in good faith and in a disinterested manner by the Whistleblower, relating to a behaviour of which the Whistleblower has had personal knowledge.
- **Collaborator:** refers to a natural person, director or member of staff of a Verallia entity, such as an employee (fixed-term contract and permanent contract), a trainee, an intern.
- **General Management:** refers to the Group General Manager, the Group Legal Director and the Group Human Resources Director.
- **Whistleblowing System:** refers to all channels and measures set up by Verallia in order to allow the reporting of all professional Alerts in compliance with this Policy. Three channels for reporting Alerts are available to Collaborators and Partners: through Hierarchical channel, through the Platform and through the Phone Line.
- **Whistleblower:** every Employee or Partner, as a natural person, who discloses or reports, in a disinterested manner and in good faith, a violation of the Anti-Corruption and Anti-Trading in Influence Policy and, more generally, a crime or an offense, a serious and manifest violation of an international engagement duly ratified by the French government, a unilateral act of an

international organization based on such an engagement, laws or regulations, or any threat or harm to the public interest, of which the Whistleblower has had personal knowledge.

- **Phone Line:** refers to the phone line enabling to issue an Alert orally. The use of the Phone Line is optional.
- **Partner:** refers to shareholders, associates, holders of voting rights in the general assembly of a Verallia entity, members of administrative, management or supervisory bodies, Verallia's external and occasional staff (interim, consultant, service provider, auditor, consultant, agent) together with a natural person or member of a legal entity having an existing or planned direct or subcontracted business relationship with Verallia (clients, suppliers, consultants, agents, intermediaries...).
- **Platform:** refers to the tool chosen by Verallia enabling to issue an Alert in writing via an external web platform. This Platform supplements, where applicable, the Phone Line and the Hierarchical channel, which also allows Collaborators and Partners to issue Alerts when possible under the applicable regulations. The use of the Platform is optional.
- **Treatment of the Alert:** refers to all the steps of the management of the Alerts, as defined in section 1.3 "Scope".
- **Verallia, the Group:** refers to Verallia S.A. (*société anonyme*), a limited company of French nationality, as well as every entity controlled by Verallia S.A.¹²
- **Hierarchical channel:** refers to any Alert reported to (i) the direct or indirect line manager of the Whistleblower or (ii) to the employer or (iii) to the compliance correspondent appointed by it or (iv) sent to the postal address mentioned in section 5 of this document.

1.3. Scope

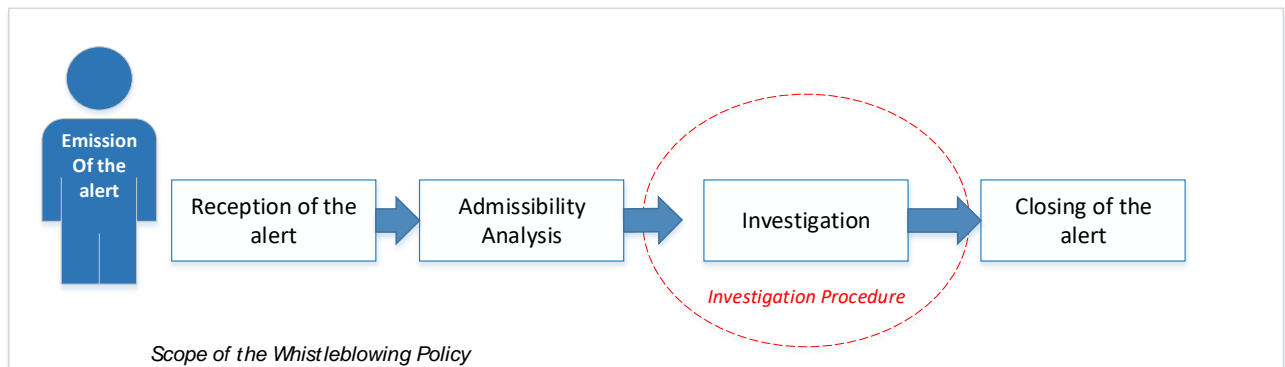
This policy applies to all Verallia Collaborators (regardless of their role, position, department) and Partners. It focuses on the Treatment of Alerts, and covers their:

- Issuance;
- Reception;
- Analysis of admissibility;
- Closing of the Alert.

¹ within the meaning of Article L. 233-3 of the French Commercial Code.

² VERALLIA S.A. controls VERALLIA PACKAGING SAS, which issued the initial version of this Policy.

The investigation of the Alerts is subject to a separate procedure (Investigation Procedure) and is not covered by this Policy.



The Whistleblowing System is based on applicable professional codes and local regulations and is required by the French law No. 2016-1691 of December 9, 2016 regarding transparency, the fight against corruption and the modernisation of the Economy (called "Loi Sapin 2") and the decree No. 2017-564 of April 19, 2017 regarding the procedures of receiving Alerts from Whistleblowers within legal entities governed by private law.

The System involves the processing of personal data, the procedures for which are described in this policy.

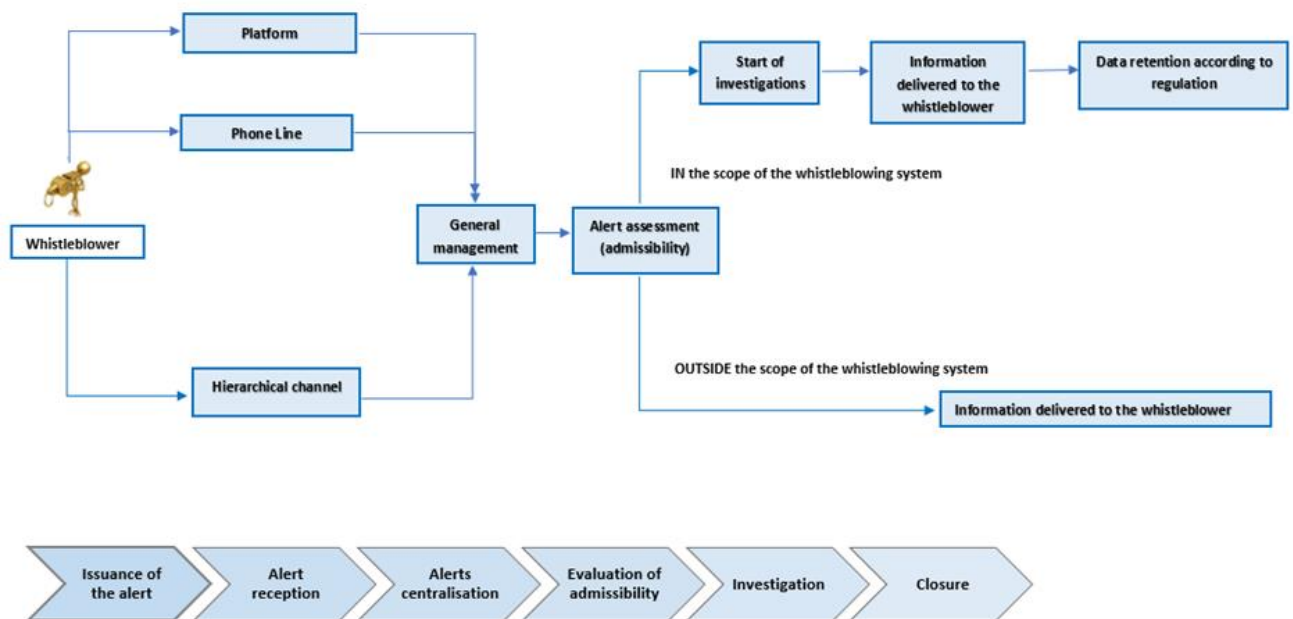
1.4. Roles and Responsibilities

The General Management:

- Centralises the Alerts and answers concerns related to the Alerts;
- Acknowledges receipt of the Alerts;
- Ensures the confidentiality of the Alerts and especially the confidentiality of the Whistleblower and the persons subject to the report;
- Ensures the analysis of admissibility of the Alerts, determining if they are within the scope described in section 2.2 and informing the Whistleblower if necessary;
- Conducts awareness campaigns on a regular basis and ensures that Verallia's values are understood and applied by all Collaborators;
- Ensures the archiving of the information and documents related to the Alerts in compliance with the applicable local regulation, particularly in terms of protection of personal data (see section 3.4 "Processing of personal data");
- Reports to the Compliance Committee on the Alerts, remediation actions and their implementation.

2. The Alerts and the Whistleblowing System

2.1. Flowchart



2.2. What should be reported?

Collaborators and Partners can report any facts related to:

- Violations of Verallia Code of Conduct and the Anti-Corruption and Anti-Trading in Influence Policy;
- Crimes or offences;
- Serious and manifest violations of an international commitment duly ratified or approved by the French government;
- Serious and manifest violations of a unilateral act of an international organisation based on such a commitment;
- Serious and manifest violations of laws and regulations;
- Or serious threats or harm to the public interest, of which the Whistleblower has personal knowledge.

As an example, the Alerts can relate to the following subjects: corruption, anti-competitive practices, discrimination, fraud, workplace harassment.

Furthermore, in case of serious and imminent danger or in presence of a risk of irreversible damage, the matter can directly be reported to the judicial or administrative authorities or the professional bodies.

However, the Alert must not relate to matters covered by military secrecy, medical secrecy or attorney-client privilege.

2.3. Who can raise an Alert?

The Whistleblower must be a Verallia Collaborator or Partner (as defined in section 1.2 “Definitions”).

Furthermore, the Whistleblower must:

- **Have personal knowledge** of the facts reported: Whistleblowing is not about reporting facts that have been observed by someone else, but reporting facts that have been personally observed and for which the Whistleblower has reasonable grounds to believe that these can be reported (according to section 2.2 “What should be reported?”).
- **Act in a disinterested manner**: The Whistleblower must act with the objective to defend the public interest and not in his/her own interest; he/she must not receive any advantage nor financial compensation in return for the report.
- **Act in good faith**: The inappropriate use of the Whistleblowing System can lead to disciplinary sanctions or judicial proceedings against their author. However, using the Whistleblowing System in good faith, even if the reported information turns out to be inaccurate or does not lead to further proceedings, will not expose the author to a disciplinary sanction.

Making use of the Whistleblowing System is a right that the persons concerned can freely exercise, its use remains optional. Therefore, not using the Whistleblowing System will not have any consequences for Collaborators.

2.4. Content and Language of Alerts

In general, and subject to locally applicable regulations, the Alert may be made anonymously or not.

However, provided that it is not prohibited under locally applicable regulations, Verallia encourages the Whistleblower to disclose their identity. In any case, the identity will be protected and treated in a strictly confidential manner according to the conditions set out in section 3.2 “Confidentiality”.

By way of exception, if the seriousness of the facts is established and the facts are sufficiently detailed, Alerts can be made anonymously.

However, anonymous reports are not encouraged and do not allow an efficient processing of the Alert.

Whistleblowers are advised to provide the facts, information and documents to support their Alert, regardless of their format. This data, which must be directly related to the subject of the report, may include the following:

- The reason for raising the Alert;
- The identity of the persons subject to the Alert;
- Each document considered necessary to support the Alert.

The wording used to describe reported facts must reflect their alleged nature.

In this context, the only Alerts that will be taken into account are those strictly limited to the facts covered by the Whistleblowing Policy, formulated in an objective manner, directly related to the scope of the Whistleblowing Policy and strictly necessary for the verification of the allegations.

Collaborators and Partners can choose in which language they would like to make the Alert. Upon receipt, the Alert can be translated into French or English if necessary.

2.5. How to raise an Alert?

Every employee must feel free to discuss about the ways to raise an Alert as well as its content.

Any question related to the interpretation of the scope of the Whistleblowing process can be discussed with the Head of Human Resources and/or the Compliance correspondent of the employing or subcontracting Verallia entity.

Three channels for reporting Alerts are available (see section 2.1 “Flow Chart”):

- **The Hierarchical channel**: provided that this is not prohibited under locally applicable regulations, the Alert can be reported (i) to the direct or indirect line manager or (ii) to the employing Verallia entity or (iii) to the Compliance correspondent appointed by it or (iv) by sending a letter to the postal address mentioned in section 5 of this document.
- **Platform**: The Alert can also be made by using the web tool (Whistleblowing Platform Convercent) available at the following link: [https:// Ethics.Verallia.com](https://Ethics.Verallia.com).
- **Phone Line**: the Alert can also be made orally by phoning free of charge to a call centre (managed by the Convercent service provider) whose contact details are available on the Platform's homepage. Oral Alerts are transcribed in writing by the call centre.

2.6. Management of Alerts

- **Centralisation of the Alerts:** Regardless of the channel used to make an Alert (Hierarchical channel, Platform or Phone Line), all Alerts are reported to the General Management:
 - If an Alert is reported by using the Hierarchical channel, the recipient of the Alert must immediately inform the Group Legal Director and the Group Compliance Officer at the following address: compliance@verallia.com ;
 - If an Alert relates to one or more members of the General Management and/or one of its shareholders, the Whistleblower or the recipient of the Alert shall directly inform the Group Compliance Officer.
- **Reception of the Alert:** If an Alert is launched via the Platform, an acknowledgement of receipt is sent via the Platform to the Whistleblower. If an Alert is launched via the Hierarchical Channel, an email acknowledging receipt is sent by the Group Legal Director or the Group Compliance Officer. In this context, it is specified that the acknowledgement of receipt does not imply the admissibility of the Alert.
- **Admissibility of the Alert:** Each Alert is subject to a preliminary analysis, is treated in a confidential manner, to determine whether the Alert falls within the scope of section 2.2 *“What should be reported?”*
 - The Alerts out of the scope of section 2.2 *“What should be reported?”* cannot be treated within the Whistleblowing System; the Whistleblower will be notified and guided towards the appropriate channels.
 - The Alerts within the scope of the Whistleblowing System will be treated in accordance with this Policy.

2.7. Investigation

If the facts reported are within the scope of the Whistleblowing System, the investigation of the Alert is carried out using means (interviews, data searches, etc.) that may vary depending on the context and the nature of the subject.

Alerts are processed by Verallia’s internal departments that need to know them, namely:

- the Triage Committee, made up of the Group General Manager, the Group Legal Director and the Group Human Resources Director;
- the Investigation Committee, made up of the Head of Investigation and the investigation team.
- the Group Compliance Committee (to the extent strictly necessary and proportionate with regard to the justification for supplying the information).

The Head of Investigation may contact the local Verallia entity to which the facts pertain, as well as various persons (employees, customers, suppliers) in order to obtain the information, data and

documents necessary to process the Alert. They may also call on the appropriate internal and/or external experts (human resources department, lawyers, chartered accountants, analysts, etc.).

For all these contacts and communications, information relating to the existence and content of the Alert is only communicated to the extent strictly necessary.

Furthermore, the wording used to describe reported facts should reflect their alleged nature. The person targeted by the Alert is presumed innocent throughout the investigations.

2.8. Communication with the Whistleblower

The Group implements all the necessary means to treat the Alerts, including by communicating with the Whistleblower in order to obtain sufficient information to analyse the reported facts.

Additional information can be requested or questions can be asked to the Whistleblower either via the Whistleblowing tool, or by communicating directly with the Whistleblower if he/she agrees to do so.

The Whistleblower is notified about the closing of the treatment of the Alert once it is completed.

3. General Principles

3.1. General

When raising an Alert, Verallia Collaborators and Partners are informed of the following principles:

- The Alerts are subject to regular reporting to the Compliance Committee;
- The Alerts are treated by persons designated for this task;
- The Whistleblowing System can only work with information communicated in “good faith”.

Verallia is committed to a non-retaliation policy; as such, no retaliatory measures shall be taken against any Whistleblower having raised an Alert in good faith (Platform, Phone Line or Hierarchical channels).

Verallia does not tolerate any form of retaliation against Whistleblowers, such as harassment. Disciplinary measures or sanctions can be taken against the author(s) of retaliations actions.

3.2. Confidentiality

The Whistleblower’s identity and that of the person subject to the Alert remains confidential throughout its treatment, in accordance with applicable laws and regulations. In such context, any person involved in the management of Alerts receives specific training and is bound to an enhanced

confidentiality obligation. These persons shall not use the data inappropriately and commit to respect the data retention period in accordance with applicable laws and regulations.

The Whistleblower must identify himself/herself, but his/her identity is treated confidentially by the organization in charge of the management of the Alerts.

Any elements that may allow to identify the Whistleblower cannot be disclosed, except to the judicial authorities and only with the consent of the Whistleblower.

Any elements that may allow to identify the person accused by an Alert cannot be disclosed, except to the judicial authorities if the Alert is followed by a legal action.

The persons in charge of the Whistleblowing Platform can also have access to the data, within the limits of their functions, for the purpose of administrating the Whistleblowing Platform.

3.3. Protection of personal data

3.3.1. Personal Data

- The Whistleblowing Alert System is implemented by Verallia SA within the Group in order to meet its legal obligations.
- Categories of data processed via the Whistleblowing Platform: Verallia is committed to only process data which is adequate, relevant and not excessive in relation to the objectives for which it is being collected. Only the following categories of data can be processed:
 - Identity, functions and contact information of the Whistleblower;
 - Identity, functions and contact information of the persons subject to an Alert;
 - Identity, functions and contact information of the persons involved in the reception or treatment of the Alert;
 - The facts that are being reported;
 - Elements of information collected during the verification of the reported fact;
 - Summary report of the verification processes;
 - Follow-up actions related to the Alert.
- **Recipients:** In addition to the persons authorised to process the data as part of their assignment, Verallia S.A. may communicate data:
 - To the group entity to which the facts relate and/or to any internal and/or external experts (human resources department, lawyers, chartered accountant, analysts, etc.) that Verallia may call on to process the Alert.
 - To the service provider(s) responsible for supplying and operating the Platform and the Phone Line.

Where applicable, data may be sent to the judicial authority, it being specified that:

- Any elements that may identify the Whistleblower can only be disclosed to the judicial authorities with the consent of the Whistleblower;
 - Any elements that may identify the person implicated by an Alert can only be disclosed if the Alert is followed by a legal action.
- **Protection measures for personal data:** Verallia S.A. takes all necessary precautions to preserve the security of the data both when it is collected and when it is communicated or stored. In this context, the data processing can only be accessed via the Platform with a user identification and an individual password that are regularly renewed, or by any other authentication method. These logins are recorded and their frequency is controlled.

3.3.2. Retention of personal data

Within the framework of the Whistleblowing System, personal data is retained according to applicable local laws and regulations and Verallia's rules and procedures on the protection and retention of personal data. In this context, personal data will be retained as follows:

- When an Alert does not fall within the scope of the Whistleblowing System (as described in section 2.2), the related data will be immediately deleted or anonymised and archived;
- When no follow-up is given to an Alert, following the closure of investigations in accordance with the laws and regulations in force³, the data are deleted or archived, after anonymisation;
- When the Alert is followed by disciplinary or judicial proceedings, data is kept until the end of the proceedings or until the lodging of any appeals against the decision;
- The data may be stored for a longer period, in temporary storage, if Verallia has a legal obligation to do so (for example, to meet accounting, social security or tax obligations).

3.3.3. Transfer of the Data outside of the European Union

For the purpose of treating the Alert, Personal data are hosted in the Platform in Europe. Nevertheless, they can be transferred (i) by Verallia to other entities of the Verallia Group or third parties registered in countries within or outside of the European Economic Area (EEA) or (ii) by the provider of the Platform and of the Phone Line for support and maintenance needs. This includes countries which do not have the same level of protection of personal data as in the EEA.

Verallia ensures that such transfers are carried out by Verallia in compliance with applicable personal data protection regulation and will be secured through adequate data privacy safeguards such as the conclusion of standard contractual clauses adopted by the EU Commission.

3.3.4. Rights of individuals

The Whistleblowing System guarantees the confidentiality and the respect of the rights throughout the treatment of Alerts.

The recipient informs the Whistleblower upon reception of the Alert.

Accordingly, the person subject to an Alert is informed that personal data is being processed as soon as the alert is registered (electronically or not). This information is delivered within one month following the Alert, unless it is likely to make impossible or seriously compromise the purposes of the processing (for example, risk of destruction of evidence relating to the Alert). In this case, the person subject to an Alert is only informed when the risk is eliminated.

Any person identified in this Policy, whether the Whistleblower or a person subject to an Alert, has the right to access his/her personal data and to request the correction or deletion of personal information if it is incorrect, incomplete, ambiguous or outdated. Any identified person may also request the rectification or erasure of their data under the conditions and limits provided for by the applicable regulations. They may also object to the processing or request its limitation. These rights may be exercised by writing to the following address: *donnees.personnelles@verallia.com*.

It should however be noted that the person subject to an Alert can under no circumstances obtain information regarding the identity of the Whistleblower, based on the right to access personal data.

If, after contacting Verallia, the data subject considers that their rights are not respected or that the processing does not comply with the data protection rules, they may lodge a complaint to the competent supervisory authority (the French Data Protection Authority (CNIL) for France).

4. Reporting to the Compliance Committee

The Group Compliance Officer reports to the Compliance Committee once a year about Alerts, management, and the actions taken in this context. This information shall be limited to that which is strictly necessary and proportional to the purpose of the communication.

5. Contacts

Entity: Verallia S.A.

Postal address: Tour Carpe Diem, 31 Place des Corolles, 92400 Courbevoie, France

For the attention of the Group Compliance Officer.

E-mail address: compliance@verallia.com

May 2022

Issued by the Group Legal Director Wendy Kool-Foulon _____

Approved by the CEO Michel Giannuzzi _____