



WHISTLEBLOWING SYSTEM POLICY

(last update: July 2026)

Table of content

1. Introduction.....	3
- 1.1. Objectives.....	3
- 1.2. Definitions.....	3
- 1.3. Scope.....	5
- 1.4. Roles and Responsibilities	6
2. The Alerts and the Internal Whistleblowing System	6
- 2.1. Flowchart related to the Internal Whistleblowing System	6
- 2.2. Which alerts should be reported?	6
- 2.3. Who can raise an Alert?.....	7
- 2.4. Content and language of Alerts	7
- 2.5. How to raise an Alert?	8
- 2.6. Management of Alerts	9
- 2.6.1. Reception and admissibility	9
- 2.6.2. Investigation	10
- 2.6.3. Communication with the Whistleblower Closure.....	10
3. General Principles	11
- 3.1. General	11
- 3.2. Protection of Whistleblowers and Facilitators	11
- 3.3. Confidentiality.....	12
- 3.4. Protection of personal data	12
- 3.4.1. Personal Data.....	12
- 3.4.2. Retention of personal data.....	13
- 3.4.3. Transfer of the Data outside of the European Union.....	14
- 3.4.4. Rights of individuals.....	14
4. Reporting to the Compliance Committee	15
5. Contacts.....	15
Appendix: LIST OF NATIONAL EXTERNAL AUTHORITIES.....	16

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 Ethics* and its *Anti-Corruption Code of Conduct*, Verallia has implemented an internal **Whistleblowing System** to comply with (i) 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") as amended by Act No. 2022-401 of March 21, 2022 and its implementing decree¹, to the French Law of 27 March 2017 on the duty of vigilance and the EU Directive 2024/1769 on corporate sustainability due diligence (hereinafter together the "**Regulations**") as well as with (ii) the Verallia Group's Code of Ethics and Anti-Corruption Code of Conduct.

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 *Ethics* and/or the *Anti-Corruption Code of Conduct*, 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 internal **Whistleblowing System** constitutes an integral part of Verallia's Compliance Program.

1.2. Definitions

- **Professional Alert /Alert** : means any report transmitted by a Whistleblower, relating to (i) a violation of the Verallia Group's Code of Ethics or Anti-Corruption Code of conduct (ii) a damage to or violation of human rights, fundamental freedoms, the health and safety of individuals, as well as of the environment. more generally, (ii) any information concerning a crime or misdemeanour, a threat or harm to the general interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France or another country whose legislation applies to Verallia, of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of a law or regulation, or a threat or harm to the general interest. When the information was not obtained in the course of professional activities, the Whistleblower must have had personal knowledge of it.
- **Authority**: means any national authority designated to receive, monitor and process External Alert, it being agreed that in the case of France this means (i) the authorities expressly authorized to collect and process an Alert, (ii) the Defender of Rights , (iii) the judicial authority or (iv) the European Union institution, body or agency competent to collect information on violations falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019. The competent National Authorities are listed in the Annex to this document.
- **Collaborator**: refers to a natural person, director or member of staff of a Verallia entity, in office or whose employment relationship has ended, such as an employee (fixed-term contract and permanent contract), a trainee, an intern or applicant for employment with Verallia when the information was obtained in the course of their relationship with Verallia.

¹ Decree no. 2022-1284 of October 3, 2022 relating to the procedures for collecting and processing whistleblowers' alerts and establishing the list of external authorities instituted by Law no. 2022-401 of March 21, 2022 to improve the protection of whistleblowers.



- **General Management:** refers to the Group CEO, the Group CSR & Legal Director and the Group Human Resources Director.
- **Whistleblowing System:** refers to all channels and measures set up by Verallia in order to enable the internal collection and processing of all professional Alerts in compliance with this whistleblowing system Policy. Three channels for reporting Alerts are available to Collaborators and Partners: through Hierarchical channel, through the Platform and through the Phone Line. The Internal Whistleblowing System is only one of several channels for reporting.
- **Disclosure:** means the provision of an Alert in the public sphere (e.g.: publication in the press, social networks) by a Whistleblower in compliance with the Regulations.
- **Facilitator:** means any natural or legal person under private, non-profit law who assists a Whistleblower in issuing an Alert or Disclosure in compliance with the Regulations and whose assistance should be confidential.
- **Verallia, the Group:** refers to Verallia S.A. (*société anonyme*), a limited company of French nationality, as well as every entity controlled² by Verallia S.A.
- **Whistleblower:** every Employee or Partner, as a natural person, who reports or discloses, without direct financial consideration and in good faith an alert.
- **Phone Line:** refers to the phone line implemented by Verallia and operated by the Service Provider enabling to issue an Alert orally. The use of the Phone Line is optional.
- **Retaliation:** means any act or omission, whether direct or indirect (including any threat or attempt), that occurs in a business context and is prompted by an Alert, an External Alert or Disclosure, and that causes or may cause undue harm to the Whistleblower.
- **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 (consultant, auditor, agent) as well as the co-contractors of a Verallia Group entity (e.g. customers, suppliers, service providers, etc.), their subcontractors or, in the case of legal entities, the members of the administrative, management or supervisory bodies of these co-contractors and subcontractors, as well as the members of their staff.
- **Person in contact with the Whistleblower:** any natural person in contact with a Whistleblower (e.g. colleagues, relatives) who is at risk of retaliatory action in the course of his or her professional activities by his or her employer, clients or recipient of his or her services.
- **Platform:** refers to the Service Provider tool chosen by Verallia enabling to collect 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.

² Within the meaning of Article L. 233-3 of the French Commercial Code

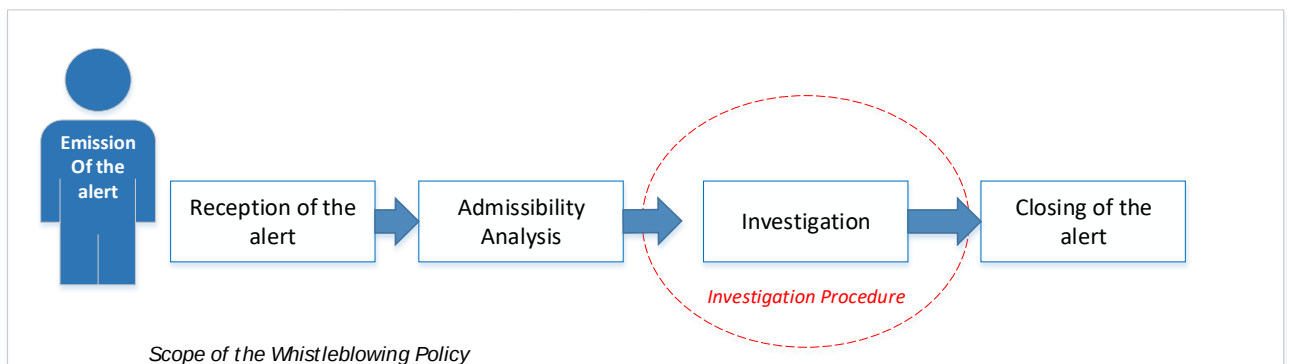
- **Service Provider:** refers to the provider that makes the Platform available to Verallia and delivers the associated services, such as the Phone Line.
- **Feedback:** means the communication to the Whistleblower of information on actions being considered or taken as follow-up and the reasons for such follow-up.
- **External Alert:** refers to the reporting of an Alert by a Whistleblower to a Competent Authority, in compliance with the regulations, either after having issued an Alert to Verallia, or directly.
- **Treatment of the Alert:** refers to all the steps of the management of the Alerts.
- **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 collection and Treatment of Alerts, and covers in particular their:

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

The procedure for investigating Alerts that must be followed by the persons in charge of processing Alerts on behalf of Verallia is the subject of a separate document (Investigation Procedure) and is therefore not covered by this Policy.



The Whistleblowing System is based on applicable professional codes and local regulations and is required by the French law.

The System involves the processing of personal data, the procedures for which are described in this policy within the 3.3 "Data protection" section.

This policy does not apply to External Alerts and Disclosures that may be made by the Whistleblower in accordance with the Regulations.

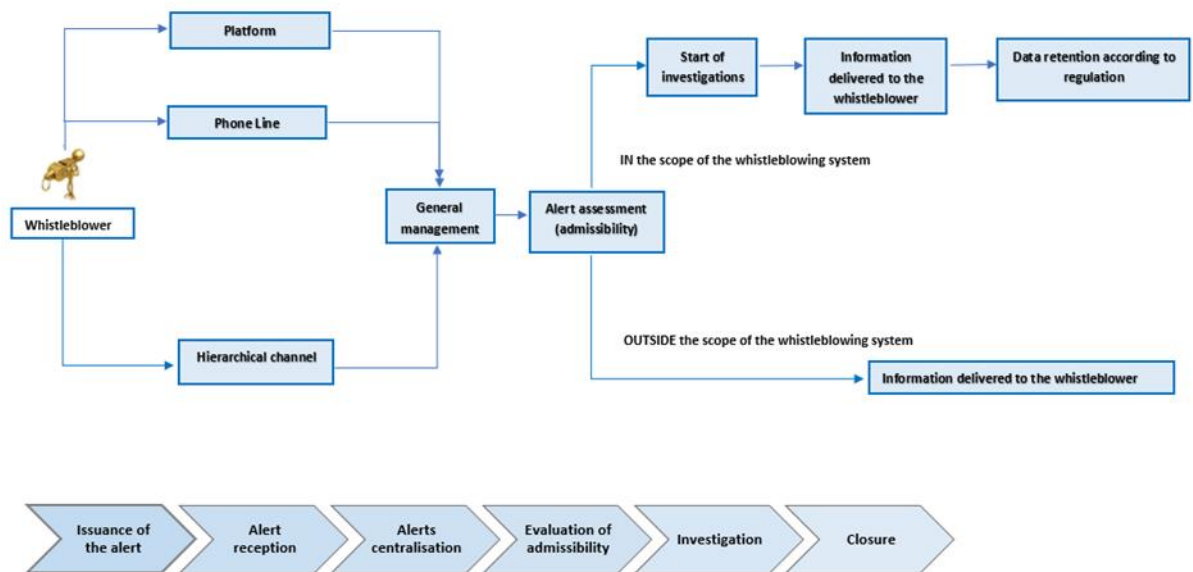
1.4. Roles and Responsibilities

The General Management:

- Receives and centralizes the alerts in accordance with Article 2.6 below;
- Acknowledges in writing receipt of the Alert to the Whistleblower within seven (7) calendar days of such receipt;
- Ensures that the Triage Committee performs the analysis of the admissibility of the Alert;
- Supervises the Investigations, ensuring that the rules are respected;
- Follows up on the measures taken following the Investigation;
- Conducts regular awareness-raising activities to ensure that Verallia's values are understood and applied by all employees and partners.

2. The Alerts and the Internal Whistleblowing System

2.1. Flowchart related to the Internal Whistleblowing System



2.2 Which alerts should be reported?

Collaborators and Partners can report any facts related to:

- Violations of Verallia Code of Ethics or the Anti-Corruption Code of Conduct ;
- Crimes or offences;
- A threat or injury to the public interest;
- A damage to or violation of human rights, fundamental freedoms, the health and safety of individuals, as well as of the environment.
- A breach or an attempt to conceal a breach of an international commitment regularly ratified or approved by France or another country whose legislation applies to Verallia;
- A breach or an attempt to conceal a breach of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of the law or of the regulations.



As an example, the Alerts can relate to the following subjects: corruption, anti-competitive practices, discrimination, fraud, workplace harassment, damage to human rights, the health and safety of individuals, damage to the environment.

Facts, information and documents, regardless of their form or medium, the revelation or disclosure of which is prohibited by provisions relating to national defense confidentiality, medical confidentiality, the confidentiality of judicial deliberations, the confidentiality of judicial investigations or proceedings, or attorney-client privilege are excluded from this Policy.

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:

- **Directly or indirectly have obtained the information in the course of his or her professional activities or, where this is not the case, had personal knowledge of it:** the Whistleblower reasonably believes that the information he or she is reporting is likely to constitute reportable information (as defined in section 2.2).

- **Act without direct financial consideration:** The Whistleblower must act with the objective to defend the public interest and not in his/her own interest. The Alert can’t be motivated by harming others.

- **Act in good faith:** The misuse 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 (or the Facilitators or Persons connected with the Whistleblower) to any Retaliatory Action.

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 and Partners.

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 his/her 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.

Furthermore, the Whistleblower is informed that in the event of an anonymous report, Verallia is not obliged to provide the feedback provided for in article 2.6.3 below.

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

- The reason for raising the Alert;



- The identity of the persons subject to the Alert;
- Any item of information in any form or medium, 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 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 English) if necessary.

Except in the case where the Alert is anonymous, the Whistleblower transmits at the same time as his alert any element justifying that he is indeed a Collaborator or a Partner.

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 “Contact” of this document.
- **Platform**: The Alert can also be made by using the web tool (by the Service Provider) available at the following link: <https://verallia.integrityline.com/>
- **Phone Line**: the Alert can also be made orally by phoning free of charge to a call centre (managed by the Service Provider) whose contact details are available on the Platform's homepage. Oral Alerts are transcribed in writing by the call centre (through the form).

When a report is received verbally, the call center verifies, unless the report is anonymous, that the author of the report is indeed an Employee or Partner and that the report falls within the scope of the Alert System. To this purpose, Verallia may request any additional information from the author of the alert.

For his or her part, the whistleblower may request the organization of a videoconference or a physical meeting of the whistleblower's choice. This videoconference or telephone meeting will be organized no later than twenty (20) days calendar after receipt of the request. Any Alert collected within this framework is subject, with the agreement of the Whistleblower, to a transcription on the Platform.

The Whistleblower can verify, rectify and approve the transcription of the Alert made on the Platform.

Subject to compliance with the imperative rules applicable locally, it is recalled that the Whistleblower also has the following reporting options:

- The Whistleblower can make an **External Alert**, either directly to an Authority or after having issued an Alert to Verallia.

This **External Alert** may be made to (i) the competent Authority, (ii) the Defender of Rights, (iii) the judicial authority, (iv) an institution, body or organization of the European Union competent to receive this Alert.

- The Whistleblower may make a **Disclosure** when the following conditions are met:
 - (i) after having made an External Alert (whether or not preceded by an Alert to Verallia), without any appropriate action having been taken in response to this External Alert at the expiration of the deadline for the Return of Information by the Authority³ or, when the Defender of Rights, the Judicial Authority or the competent European Union institution, body or agency has been seized, at the expiration of a period of six (6) months⁴;
 - (ii) in case of serious and imminent danger⁵;
 - (iii) Or where referral to an Authority would put the Whistleblower at risk of Retaliatory Action or would not effectively address the subject matter of the disclosure, due to the particular circumstances of the case, including where evidence may be withheld or destroyed or where the Whistleblower has substantial reason to believe that the Authority may have a conflict of interest in collusion with the instigator of the facts or involved in these facts.⁶

2.6. Management of Alerts

2.6.1 Reception and admissibility

- **Centralisation of the Alerts:** Regardless of the channel used to make an Alert to Verallia (Hierarchical channel, Platform or Phone Line), all Alerts are reported to the General Management and treated through the Platform:
 - If an Alert is reported by using the Hierarchical channel, the receiver of the Alert has to immediately report the Alert on the Platform; in the event of technical difficulties, the Alert should be transmitted to the Group CSR and 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.

³ 3 months (from the acknowledgement of receipt of the alert by the Authority or, in the absence of such acknowledgement, from the expiration of a period of 7 calendar days following the alert) or 6 months if the circumstances so require.

⁴ From the acknowledgement of receipt of the report or, in the absence of acknowledgement of receipt, from the expiration of a period of 7 calendar days following the report.

⁵ This condition does not apply, however, (i) to a Whistleblower who publicly discloses information obtained in the course of his or her professional activities in cases of imminent or obvious danger to the public interest, in particular where there is an emergency situation or a risk of irreversible harm, or (ii) where the public disclosure is prejudicial to the interests of national defense and security.

⁶ This condition does not apply, however, when the public disclosure affects the interests of national defense and security.

- **Receipt of the Alert:** If an Alert is launched via the Platform or the Telephone Line, an acknowledgement of receipt is sent via the Platform to the Whistleblower. If an Alert is launched via the hierarchical channel, an email of receipt is sent by the Group CSR and Legal Director or the Group Compliance Officer. In all cases, this acknowledgement of receipt is sent in writing within seven (7) calendar days of receipt. In this respect, it is specified that the acknowledgement of receipt does not constitute the admissibility of the report.
- **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 *“Which alerts 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.

The Whistleblower is informed of the reasons why Verallia considers that the Alert is not admissible. The non-receivable Alert is anonymized without delay.

2.6.2 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 CEO, the Group CSR & Legal Director, the Group Human Resources Director and the Group Compliance Officer;
- 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 concerned by the facts, 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 (internal audit department, 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.

2.6.3 Communication with the Whistleblower - Closure

Verallia implements all the necessary means to treat the Alerts within a reasonable delay, 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.

Verallia shall provide the Whistleblower with feedback (in particular with regard to the closure of the investigation of the Alert) within a reasonable period of time, not exceeding three (3) months from the acknowledgement of receipt of the Alert or, in the absence of an acknowledgement of receipt, three (3) months from the expiration of the period of seven (7) calendar days following the Alert. In this respect, Verallia will provide the Whistleblower with written information on the measures planned or taken to assess the accuracy of the allegations and, if applicable, to remedy the subject of the alert, as well as the reasons for such measures.

The Whistleblower is notified by writing about the closing of the treatment of the Alert.

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. In any case, these people have the competency, the authority and the means to carry out their missions;
- The Whistleblowing System can only work with information communicated in “good faith”.

3.2 Protection of Whistleblowers and Facilitators

The Whistleblower is reminded that, subject to locally applicable regulations:

- He or she **is not under civil liability** for damages caused by his or her reporting or disclosure if the reporting was done in accordance with the applicable provisions and the Whistleblower had reasonable grounds to believe, when he or she did so, that the reporting or public disclosure of all such information was necessary to protect the interests at stake.
- He or she **is not criminally liable**⁷ for obtaining or accessing publicly reported or disclosed information, provided that such obtaining or accessing does not constitute an autonomous criminal offence under the locally applicable regulations. In the event that such obtaining or access constitutes a separate criminal offence, the locally applicable rules of criminal liability shall apply.
- That he or she **shall not be subject to any Retaliatory Action** for reporting or disclosing information in compliance with the Regulations.

Verallia does not tolerate any form of retaliation, threats or attempts to use such measures against Whistleblowers, such as harassment.

⁷Under French law, pursuant to Article 122-9 of the Penal Code, “A person who breaches a secret protected by law shall not be criminally liable, provided that such disclosure is necessary and proportionate to the safeguarding of the interests in question, that it is made in compliance with the conditions for reporting defined by law and that the person meets the criteria for the definition of a whistleblower set out in Article 6 of Law No. 2016-1691 of December 9, 2016 on transparency, combating corruption and modernizing economic life.

Nor shall a whistleblower be criminally liable if he or she removes, misappropriates or conceals the documents or any other material containing the information of which he or she has lawfully become aware and which he or she reports or discloses under the conditions mentioned in the first paragraph of this article.

The present article is also applicable to the accomplice of these offences.

The Facilitators as well as the Persons connected with the Whistleblower and the legal entities controlled by the Whistleblower or for which he or she works, are included in Verallia's non-retaliation policy and benefit from the same protections as the Whistleblower.

Disciplinary proceedings or civil or criminal sanctions may be taken against the perpetrator of such retaliation or against any person who does not respect the Whistleblower's rights.

3.3 Confidentiality

The Processing of the Alert is carried out while respecting **integrity and confidentiality** of the information collected in the Alert, notably the identity of the Whistleblower, as well as that of the persons concerned by the Alert and of any third parties mentioned therein in accordance with the applicable law.

In this respect:

- The persons designated to handle Alerts are the persons mentioned in article 2.6.2 and 3.4.1 of this document. Access to the information collected in the framework of the Alert is forbidden to any person not authorized to know it.
- All persons involved in the management of Alerts are specially trained and bound by a reinforced obligation of confidentiality. In particular, they undertake not to use the data for improper purposes and to respect the limited period of retention of data in accordance with the applicable law.
- The Whistleblower is encouraged to identify himself, but his identity is treated confidentially by the organization in charge of managing the Alerts.
- Identifying information may only be disclosed with the Whistleblower's consent⁸.
- The elements likely to identify the person involved in an alert shall not be disclosed, except to the judicial authority, once it has been established that the alert is well founded.

Within the limits of their attributions, the persons in charge of the Platform can also access the data for the purposes of administration of the Platform.

3.4 Protection of personal data

3.4.1 Personal Data

- The Whistleblowing Alert System is implemented by Verallia SA within the Group in order to meet its legal obligations and in the legitimate interest of Verallia to conduct its business with integrity and ethics with regard to matters covered by the Code of Ethics and the Anti-Corruption Code of Conduct.
- 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;

⁸ They may, however, be communicated to the judicial authorities, in the event that the persons responsible for collecting or processing the Alerts are required to report the facts to the judicial authorities (for example: sexual assault or abuse inflicted on (i) a minor or (ii) a vulnerable person (due to illness, infirmity, physical or mental deficiency, or pregnancy)). The whistleblower is then informed, unless such information would jeopardize the legal proceedings. Written explanations are attached to this information.

- Identity, functions and contact information of the persons subject to and/or mentioned in 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, internal audit director, lawyers, chartered accountant, analysts, etc.) that Verallia S.A. may call on to process the Alert (investigation and/or processing of actions taken on 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 Whistleblower⁹;
 - Any elements that may identify the person involved in an Alert can only be disclosed once it has been established that the Alert is founded.
- **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 by Verallia S.A. 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.

3.4.2 Retention of personal data

Within the framework of the Whistleblowing System:

- The recordings, transcripts and documents are kept for the time necessary to process the alert and to protect their authors, the persons they refer to and the third parties they mention, in accordance with the applicable regulations and Verallia's rules and procedures regarding protection and storage.
- In this context, personal data is stored in the following manner:
 - When an Alert is considered not to fall within the areas described in section 2.2 "What alerts to report", the Alert is closed and the data concerning it is anonymized without delay;
 - When no action is taken on an Alert, the data is archived after the closure of the verifications according to the laws and regulations in force until the expiry of the applicable limitation period or the exhaustion of all avenues of appeal, or, where applicable, for the time necessary to conduct any additional investigations or to enable Verallia to comply with its legal obligations or with requests from the authorities. When action is taken on the alert (i.e., any decision taken by Verallia to draw consequences from the alert, such as an internal action plan, adoption or modification

⁹ Except as provided in footnote 8 above.

of internal rules, reorganization of operations or services, pronouncement of a sanction, implementation of legal action, etc.), the data relating to the alert is kept until the end of the procedure and/or until the statute of limitations has expired or all avenues of recourse have been exhausted

- The data may be kept longer, in archiving involving restricted access, if Verallia is legally obliged to do so (for example, to meet accounting, social or tax obligations) “or for evidentiary purposes in the context of a potential audit or litigation, or for the purpose of carrying out quality audits relating to the processing of reports

3.4.3 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) for the purpose of handling the Alert or (ii) by the Service Provider for service-related support and maintenance purposes. This may include 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.

Additional information regarding transfers outside the EEA is available to individuals upon request (to donnees.personnelles@verallia.com).

3.4.4 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 according to the Procedure. Accordingly, the person subject to an Alert is informed that his/her personal data is being registered (electronically or not). This information is delivered within one month following the issuing of the Alert, unless it is likely to make impossible or to 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 Whistleblowing System, whether the Whistleblower or a person subject to an Alert, has the right to access his/her personal data. Any identified person may also request the rectification or erasure of their data under the conditions and limits provided for by the applicable regulations. He/she may also object to the processing or request its limitation.

With regard to the right to object, this right may be exercised only when the processing activities relate to a violation of the Code of Ethics or the Anti-Corruption Code of Conduct (since such right is not applicable when the processing activities is performed to comply with a legal obligation by Verallia such as the Regulations).

With regard to the rights of rectification and erasure, these may not allow the retroactive modification of the elements contained in an alert or collected during its investigation. These rights may only be exercised to rectify factual data whose material accuracy can be verified by Verallia S.A. with evidence and without erasing or replacing the data, even if erroneous, initially collected.



The right of erasure is not applicable if the processing activities are necessary to comply with a legal obligation or for the establishment, exercise, or defense of legal claims.

These rights may be exercised at 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 at least 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.

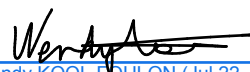
Postal address: Tour Carpe Diem, 31 Place des Corolles, 92400 Courbevoie, France

For the attention of the Group Compliance Officer.

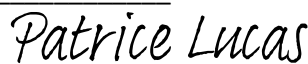
E-mail address: compliance@verallia.com

July 2026

Issued by the Group CSR Director & General Counsel Wendy Kool-Foulon


[Wendy KOOL FOULON \(Jul 22, 2026 18:16:09 GMT+2\)](#)

Approved by the CEO Patrice Lucas


[Patrice Lucas \(Jul 22, 2026 18:51:23 GMT+2\)](#)

APPENDIX: LIST OF NATIONAL EXTERNAL AUTHORITIES

1. FRANCE

1.1. Marchés publics :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;
- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;
- Autorité de la concurrence, pour les pratiques anticoncurrentielles ;

1.2. Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme :

- Autorité des marchés financiers (AMF), pour les prestataires en services d'investissement et infrastructures de marchés ;
- Autorité de contrôle prudentiel et de résolution (ACPR), pour les établissements de crédit et organismes d'assurance ;

1.3. Sécurité et conformité des produits :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF);
- Service central des armes et explosifs (SCAE) ;

1.4. Sécurité des transports :

- Direction générale de l'aviation civile (DGAC), pour la sécurité des transports aériens ;
- Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT), pour la sécurité des transports terrestres (route et fer) ;
- Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA), pour la sécurité des transports maritimes ;

1.5. Protection de l'environnement :

- Inspection générale de l'environnement et du développement durable (IGEDD) ;

1.6. Radioprotection et sûreté nucléaire :

- Autorité de sûreté nucléaire (ASN) ;

1.7. Sécurité des aliments :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER);
Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

1.8. Santé publique :

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;
- Agence nationale de santé publique (Santé publique France, SpF) ;
- Haute Autorité de santé (HAS) ;

- Agence de la biomédecine ;
- Etablissement français du sang (EFS) ;
- Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ;
- Inspection générale des affaires sociales (IGAS) ;
- Institut national de la santé et de la recherche médicale (INSERM) ;
- Conseil national de l'ordre des médecins, pour l'exercice de la profession de médecin ;
- Conseil national de l'ordre des masseurs-kinésithérapeutes, pour l'exercice de la profession de masseur-kinésithérapeute ;
- Conseil national de l'ordre des sages-femmes, pour l'exercice de la profession de sage-femme ;
- Conseil national de l'ordre des pharmaciens, pour l'exercice de la profession de pharmacien ;
- Conseil national de l'ordre des infirmiers, pour l'exercice de la profession d'infirmier ;
- Conseil national de l'ordre des chirurgiens-dentistes, pour l'exercice de la profession de chirurgien-dentiste ;
- Conseil national de l'ordre des pédicures-podologues, pour l'exercice de la profession de pédicure-podologue ;
- Conseil national de l'ordre des vétérinaires, pour l'exercice de la profession de vétérinaire ;

1.9. Protection des consommateurs :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

1.10. Protection de la vie privée et des données personnelles, sécurité des réseaux et des systèmes d'information :

- Commission nationale de l'informatique et des libertés (CNIL) ;
- Agence nationale de la sécurité des systèmes d'information (ANSSI) ;

1.11. Violations portant atteinte aux intérêts financiers de l'Union européenne :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;
- Direction générale des finances publiques (DGFiP), pour la fraude à la taxe sur la valeur ajoutée ;
- Direction générale des douanes et droits indirects (DGDDI), pour la fraude aux droits de douane, droits anti-dumping et assimilés ;

1.12. Violations relatives au marché intérieur :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;
- Autorité de la concurrence, pour les pratiques anticoncurrentielles et les aides d'Etat ;
- Direction générale des finances publiques (DGFiP), pour la fraude à l'impôt sur les sociétés ;

1.13. Activités conduites par le ministère de la défense :

- Contrôle général des armées (CGA) ;
- Collège des inspecteurs généraux des armées ;

1.14. Statistique publique :

- Autorité de la statistique publique (ASP) ;

1.15. Agriculture :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

1.16. Education nationale et enseignement supérieur :

- Médiateur de l'éducation nationale et de l'enseignement supérieur ;

1.17. Relations individuelles et collectives du travail, conditions de travail :

- Direction générale du travail (DGT)

1.18. Emploi et formation professionnelle :

- Délégation générale à l'emploi et à la formation professionnelle (DGEFP) ;

1.19. Culture :

- Conseil national de l'ordre des architectes, pour l'exercice de la profession d'architecte ;
- Conseil des maisons de vente, pour les enchères publiques ;

1.20. Droits et libertés dans le cadre des relations avec les administrations de l'Etat, les collectivités territoriales, les établissements publics et les organismes investis d'une mission de service public :

- Défenseur des droits ;

1.21. Intérêt supérieur et droits de l'enfant :

- Défenseur des droits ;

1.22. Discriminations :

- Défenseur des droits ;

1.23. Déontologie des personnes exerçant des activités de sécurité :

Défenseur des droits.