

## Protection of personal data within the scope of the Whistleblowing system of Verallia Group

### Prior information for users of the Platform

*Terms beginning with a capital letter are defined in the Verallia Whistleblowing system Policy - or in the Whistleblowing system User Guide.*

In accordance with our values of **respect for people, laws and the environment**, and as part of the implementation of initiatives supporting our Code of Ethics and its Anti-Corruption Code of Conduct, Verallia has put in place a 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 decree, 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 Collaborators and Partners to report in a disinterested manner and in good faith actions of which they have personal knowledge that potentially contradict the legal obligations or the Code of Ethics and/or the Anti-Corruption Code of Conduct, under the conditions defined by the Whistleblowing Policy.

Within this scope and in order to comply with its legal obligations, Verallia S.A. collects and processes, as Controller, the information needed to analyze and act on Alerts concerning:

- Violations of the Code of Ethics and/or the Anti-Corruption Code of Conduct;
- Crimes or offences;
- Clear and manifest violations of international commitment duly ratified or approved by The French government;
- A damage to or violation of human rights, fundamental freedoms, the health and safety of individuals, as well as of the environment
- Serious and manifest violations of unilateral act of an international organization based on such a commitment;
- Serious and manifest violations of laws or regulations;
- Or serious threats or harm to the public interest, that the Whistleblower has personal knowledge.

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.

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 (reason for raising the Alert, identity of individuals concerned, any document deemed necessary to substantiate the Alert). **Verallia draws the attention of whistleblowers to the fact that reports must remain factual and have a direct link with the subject of the report.**

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.

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

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.

Alerts are processed by:

- The internal departments of Verallia which need to know them, namely:
- the Triage Committee, composed by the Group General Manager, the Group Legal Director and the Group Human Resources Director;
- the Investigative Committee, comprising the Head of Investigations and the investigation team, if appointed.
- the Group Compliance Committee (to the extent strictly necessary and proportionate with regard to the justification for supplying the information).
- 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 S.A. may call on to process the Alert (investigation and/or processing of actions taken on the alert)..
- In case of disciplinary proceedings, the Human Resources Department of the Company which is the employer of the employee subject to these proceedings has to be involved.
- 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, 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.

Personal data are hosted within the Platform in Europe. However, 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 purposes of processing of the Alert or (ii) by the service provider responsible for the Platform and Phone Line for the purposes of providing the services, notably support and maintenance. 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 by Verallia are carried out in compliance with applicable local 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](mailto:donnees.personnelles@verallia.com)).

Verallia S.A. takes all the necessary precautions to preserve the security of the data both during their collection and their communication or storage.

Within the Whistleblowing System, personal data is kept in compliance with applicable local legislation as well as Verallia rules and procedures regarding data protection and retention. In this regard, personal information is retained in the following ways:

- When an Alert does not fall within the scope of the Whistleblowing System 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 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

Any person whose data are processed within the scope of the Whistleblowing system, 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. They 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 by writing to the following address: [donnees.personnelles@verallia.com](mailto:donnees.personnelles@verallia.com).

For more information regarding the Whistleblowing System, please see the Verallia Whistleblowing System Policy or the Whistleblowing system User Guide.

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).