

Whistleblowing Policy

External version

Ethics & Compliance / Version 2.0 | 03.2025



Document Management

Version	Date	Key Updates
1.0	01/01/2024	Creation
2.0	01/03/2025	Modifications on the overall policy
Modified by:	Group Ethics & Compliance Department	
Approved by:	Chief Legal Officer and General Counsel	

Table of Contents

1. Introduction	3
1.1 Purpose	3
1.2. Scope of application of the policy	3
1.3 Local adaptations	3
2. Definitions	4
3. Governance – speak up ethics committee	5
4. Who can speak up?	6
5. When to speak up?	6
6. Strict confidentiality obligation	7
7. Non retaliation	8
8. How to speak up?	9
8.1 Speak up tool	9
8.1.1. Speak up tool website	9
8.1.2. Levels of anonymity	9
8.2 Other channels	10
9. Management of alerts and investigation	11
9.1 Receipt of the alert	11
9.2 Alert assignment	11
9.2.1 Principle of escalation	11
9.2.2. Absence of conflict of interest	11
9.2.3 Non-disclosure agreement	12
9.3 Timeline and notification	12
9.4 Investigation organization	12
9.5. Content of an investigation	12
9.6. Termination of the alert	12
10. Archiving and data protection obligations	14

1. Introduction

1.1 Purpose

Pluxee Group, composed of Pluxee International and all its subsidiaries ("Pluxee"), is committed to conducting business according to Pluxee's values and ethical principles, without corruption or conflict of interests or unfair competition, whilst eliminating all forms of discrimination, harassment or compulsory labour and ensuring that slavery and human trafficking do not take place in any part of the business or supply chain.

This policy (referred to as the "Policy") aims to establish the standards and procedures for reporting alleged violations of the Pluxee's Ethics Charter. It also provides a framework to promote a responsible and secure environment for employees and stakeholders without fear of retaliation.

Pluxee expects all employees to maintain high standards in accordance with these principles and with Pluxee's Ethics Charter. Those who work for and with Pluxee should always be respected and confident about the integrity of their relationship and engagement with Pluxee.

The aims of this Policy are:

- To encourage everyone to report suspected wrongdoings as soon as possible, in the knowledge that their allegations will be taken seriously and appropriately investigated.
- To provide guidance on how to raise those allegations.
- To explain the functioning of the whistleblowing tool ("Speak Up"), which guarantees their confidentiality and provides the option of anonymity (when applicable and permitted under local laws).
- To reassure everyone that they can raise genuine allegations without fear of retaliation, even if they turn out to be mistaken.

1.2. Scope of application of the Policy

This policy applies to all Pluxee employees, consultants, contractors, casual workers, intermediaries (e.g., lobbyists, public affairs specialists, etc.), external or occasional collaborators (e.g., temporary staff, interns, service providers, employees of subcontracting companies, etc.), working for any Pluxee entities.

1.3 Local adaptations

This Policy derives from the core ethical principles outlined in Pluxee Ethics Charter.

While this Policy establishes strategic-level guidelines, the Local Compliance Function may develop provisions adapted to local operational needs and put in place additional procedures tailored to each Pluxee Entity's needs.

2. Definitions

Case Review Team	means the persons assigned to manage/investigate an alert. There are three types of Case Review Team to review alerts whilst respecting the escalation process: local ones, "Speak Up Champion", Regional level and Global level
EXCOM	means Executive Committee
Local	means the level or scope related to a Pluxee Entity, such as a local function (e.g. Compliance, Procurement, Finance, etc.)
Function	means a specific department or area of responsibility within Pluxee Group, such as Compliance, Procurement, Finance, Legal, or other similar departments, each managing distinct operational or strategic activities
Global	means the level or scope related to Pluxee Headquarters or Pluxee Group as a whole, covering all regions and entities worldwide and managed centrally
Pluxee	means all entities of Pluxee Group, including Pluxee N.V., Pluxee International and all of Pluxee entities unless otherwise specified
Pluxee Entity	means any subsidiary or affiliate, or other company directly or indirectly controlled by, or under common control with Pluxee International
Pluxee Headquarters	means Pluxee International
Regional	means the level or scope related to a Pluxee Region, as defined in the geographical governance structure (France, Brazil, Hispanic Latin America, UK & US, Asia, Middle East, Africa & Continental Europe)
Speak Up tool	means the whistleblowing alert system platform accessible here
Speak Up Champion	means any person assigned at local level, in a Pluxee entity, to be in charge of managing and investigating local alerts (when applicable)
Unique access code	means the code received when a Whistleblower wants to access its alert on Speak Up tool website
Whistleblower	means a physical person who raises a genuine allegation, without direct financial gain and in good faith, relating to any breach that meets the conditions of admissibility listed hereunder in chapter 5

3. Governance – Speak Up Ethics Committee

The Speak Up Ethics Committee meets to:

- monitor all new alerts,
- decide to carry-out an investigation from an alert,
- follow-up on the progress of the alert review and investigation if any of each relevant alert.

4. Who can speak up?

Definition of Whistleblower:

A Whistleblower is a physical person who raises a genuine allegation, without direct financial gain and in good faith, relating to any breach that meets the conditions of admissibility listed hereunder in chapter 5.

Anyone can make allegations provided that they comply with the criteria referred to above.

This includes anybody working directly or indirectly for Pluxee International or local Pluxee Entities, even after the end of their relationship if the relevant information subject to the alert was obtained during this relationship, and anybody applying for employment within the entity concerned, where the alleged behaviour complained of occurred in the context of that application.

5. When to speak up?

Admissibility conditions on the allegation:

The following type of allegations can be reported under the whistleblowing system, whether past, present or highly likely to occur:

- **Conduct or situations in violation of the Ethics Charter and/or Pluxee policies,**
- **A crime or an offense,**
- **A breach of law or regulations,**
- **A threat of or serious damage to the public interest.**

Individual dysfunctions – such as process inefficiency – alone do not provide sufficient ground for issuing an alert.

The admissibility of each allegation is verified before the allegation is submitted to the corresponding Case Review Team.

The Whistleblower will be informed of the reasons why the Case Review Team, if applicable, considers that the allegation does not meet the conditions mentioned above.

6. Strict confidentiality obligation

Anyone who is made aware of an allegation, which includes the Speak Up Ethics Committee, and the different Case Review Teams assigned to review and/or investigate the alert, is subject to strict obligation of confidentiality and information integrity.

Should anyone wish to raise allegations, Pluxee is bound to ensure strict confidentiality regarding identities and determining characteristics.

All parties involved including the accused, the Whistleblower and any third parties mentioned in the alert, are entitled to strict confidentiality to avoid unnecessary reputational damage. Therefore, a Whistleblower participating in or learning about an investigation must keep the matter strictly confidential.

More specifically, information relating to the identity of the Whistleblower may not be disclosed without his/her consent except if requested by a judicial authority of which the Whistleblower is informed, unless it could jeopardize the legal proceedings.

Information relating to the identity of the accused cannot be disclosed, except to a judicial authority, until the alert has been confirmed as well-founded.

Any information provided by Pluxee must remain confidential throughout and after the investigation and is only shared on a need-to-know basis.

7. Non retaliation

The Case Review Team assigned to an alert is responsible for ensuring the proper implementation of this Policy so that employees and stakeholders can raise allegations without fear of retaliation.

This requires the members of the Case Review Team:

- to act impartially when managing and/or investigating an alert,
- to not jump to easy conclusions,
- to verify the absence of retaliation against the Whistleblower after the investigation.

Therefore, the applicable Case Review Team in charge of the alert must address employee concerns and questions regarding ethics or wrongdoing at every step of the investigation/review.

In the event of retaliation, the affected person must submit a new alert through the Speak Up tool.

Protection against retaliation is also extended to (i) facilitators (i.e., any individual or private, non-profit legal entity that helps the Whistleblower to report an alert), (ii) individuals associated with the Whistleblower (i.e. anyone who could, in the course of their professional activities, suffer retaliation from the employer, their customer or the recipient of their services), and (iii) legal entities the Whistleblower works for or with which they have a professional relationship or which they control.

In instances of misuse of the tool by raising abusive allegations or making deliberately false accusations with the intent to cause harm, such actions shall not qualify the author of the alert as a Whistleblower, as defined and protected by law and this Policy and may expose the author of the alert to disciplinary sanctions and legal proceedings.

8. How to Speak up?

Pluxee provides multiple accessible channels for raising an allegation:

- An online whistleblowing platform: the Speak Up tool (8.1),
- All other means including email address and human channels (e.g., the line management and Speak Up champions) (8.2).

Pluxee ensures that all allegations, regardless of the method of communication, are managed with the same guarantees.

8.1 Speak Up tool

8.1.1. Speak Up tool website

The Speak Up tool is run by an independent third party and is available 24/7, 365 days a year, in 60 languages.

To submit an alert through the Speak Up tool, the Whistleblower should file a report online, on Speak Up tool's website <http://www.pluxeespeakup.com>.

When raising an allegation, the Whistleblower should provide as many details as possible to enable a proper assessment and investigation, such as: background, history and the reason for the concern, documentation, etc.

The Speak Up tool is not an emergency hotline or a substitute for contacting law enforcement. A Whistleblower facing a life-threatening emergency or who believes they face the threat of imminent bodily harm, must contact the local police or emergency telephone number immediately.

8.1.2. Levels of anonymity

The Speak Up tool offers three options to raise an allegation:

Level of anonymity:	Pure anonymity	Semi-anonymity	No anonymity
Level of information on the Whistleblower:	No information required	Email address only	Name
Notification to the Whistleblower on the alert's management progress	Whistleblower can only see the progress by connecting to Speak Up with a Unique Access Code	Notification received on the email address registered through Speak Up	Notification received on the email address registered and through Speak Up
Communication channel	Speak Up communication channel only	Speak Up communication channel and email address provided by the Whistleblower	Speak Up communication channel or any other means (meetings, calls, teams meeting....)

Nota Bene: The Whistleblower has the possibility to remain strictly anonymous, nonetheless, disclosing allegations which are made on a non-confidential basis eases communications during the management of the alert.

Unique Access Code

If an alert is made anonymously through the Speak Up tool, the Whistleblower will receive a "Unique Access Code". It can be used to access the Speak Up tool to check the progress on the alert.

The Whistleblower will also be able to see whether the person in charge of managing the alert has any feedback or further questions. The Whistleblower can provide additional information.

When opting out from email notifications, the Whistleblower can only view updates relating to the alert by logging in, using its Unique Access Code to the Speak Up tool.

8.2 Other channels

In case of use of other channels, all allegations raised by the Whistleblower must be handled accordingly to this procedure, be in line with the defined requirements, and must be recorded in the Speak Up tool whilst respecting the level of anonymity chosen by the Whistleblower.

- Pluxee Group provides an email address to anyone who wants to report an allegation, by sending an email to the following address: **speakup.group@pluxeegroup.com**.
- When allegations are received by phone call or in conversation, the Whistleblower must give his/her consent in order for the conversation to be recorded or for it to be documented in writing.

Any evidence, such as emails, alerts resulting from controls (e.g., internal or external audits, internal control campaigns), or discussions about a concern must be recorded in the Speak Up tool and in accordance with the decision and investigation processes defined by Pluxee International.

When applicable and allowed by local laws, the Whistleblower may also report to a judicial or administrative authority, professional body or any other relevant institution or body.¹

¹ Under French law, Whistleblowers may also report the alert to:

- (i) The "Défenseur des droits" (https://formulaire.defenseurdesdroits.fr/formulaire_saisine/);
- (ii) A judicial authority;
- (iii) One of the competent authorities listed in the appendix to Decree No. 2022-1284 of October 3, 2022, relating to the procedures for collecting and processing reports issued by whistleblowers and establishing the list of external authorities established by Law No. 2022-401 of March 21, 2022, aimed at improving the protection of whistleblowers (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368>);
- (iv) An institution, body, office or agency of the European Union competent to receive information on breaches falling within the scope of the aforementioned Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019.

9. Management of Alerts and investigation

All alerts must be recorded in the Speak Up tool. After receiving the Speak Up alert, the Pluxee International Case Review Team verifies its admissibility (9.1). Once confirmed, the alert is assigned in application of the following organization (9.2), in line with the mandatory management periods and notification obligation (9.3).

9.1 Receipt of the alert

Once an alert has been made on the Speak Up tool, an acknowledgement of receipt is sent to the author of the alert within **seven working days**.

Verification of admissibility: each alert's admissibility is verified before its assignment to the corresponding Case Review Team, under the criterion provided in this Policy in chapter 4 and 5.

- In case of non-admissibility, the alert is closed, and its author is duly informed of the reasons why the alert does not meet the conditions mentioned above.
- In case of admissibility, the alert is assigned to the appropriate Case Review Team for its management (6.2).

9.2 Alert assignment

9.2.1 Principle of escalation

There are different levels of actors that oversee the management of alerts, depending on the subject and the position of the persons reported and/or involved in the alert. The escalation process aims at providing the Case Review Team members with knowledge and awareness to determine who will handle the investigation and who will be the decision maker.

When a member of the Case Review Team is reported in an allegation, it must be reviewed and investigated by the Case Review Team members of the upper level.

- Case review team at Global level - "Pluxee International Case Review Team": this team oversees assigning alerts to the appropriate "case review team" at local or regional or Pluxee International level, when applicable.
- Case review team at regional level: this team oversees alerts in cases where any reported or involved parties are local top management.
- Case review team at local level - "Speak Up Champion": this team is composed at least by local HR and/or Compliance and/or Legal manager assisted by any relevant local function depending on the allegations raised and functions reported.

9.2.2. Absence of conflict of interest

Members of the Case Review Team must voluntarily step-out or not be involved in any part of the process, if he/she deems that managing the alert shall create a conflict of interest.

9.2.3 Non-Disclosure Agreement

Any person involved in the investigation/management of an alert must sign a non-disclosure agreement to ensure strict confidentiality obligations.

9.3 Timeline and notification

The Case Review Team will formally communicate to the Whistleblower, within:

- **three months** from the acknowledgment of receipt of the report or,
- in the absence of an acknowledgment of receipt, **three months** from the expiration of a seven working day period following the date the report is made.

This communication must outline information on the measures planned or taken to assess the accuracy of the allegations and, if applicable, to address the subject of the alert, as well as the reasons for these measures.

9.4 Investigation organization

To conduct a thorough investigation, the Case Review Team responsible for the management of an alert may require the assistance of internal employees with specific expertise (e.g., legal, human resources, internal audit, investigation, security) as well as external firms specializing in forensic investigation and law firms. As provided under section 6, information related to an alert shall be shared only on a need-to-know basis.

In any case, the investigation can be performed with the help of an external law firm or forensic investigation firm to ensure proper independence.

9.5. Content of an investigation

Alerts will undergo an initial review by the appropriate Case Review Team, and if necessary, will be investigated. To assess the accuracy of the allegations made, the Case Review Team may request additional information from the Whistleblower.

If the allegations appear to be substantiated, the Case Review Team will take the necessary measures to address the person against whom the allegations are made of in the alert. When investigating, the Case Review Team is permitted to conduct interviews, and have access to all professional information (e.g., access to emails, Teams messages, etc. ...)

The Whistleblower will be duly informed of the findings. However, full details of the outcome of a case (or related actions taken) must remain confidential to preserve privacy and the legal rights of all concerned.

All investigations must be documented and follow the investigation template provided by Pluxee Group on a case-by-case basis.

9.6. Termination of the alert

After the investigation of the alert and regardless of the findings, the alert must be marked at closed in the Speak Up tool. The Whistleblower must be formally and timely notified that the alert has been closed.

10. Archiving and data protection obligations

- **Inadmissible, unfounded or incomplete alerts** (i.e. alerts that are not investigated by the Ethics & Compliance team) are archived within a maximum of **two months** after their completion and then deleted no later than **five years** after, in accordance with legal and regulatory obligations.
- **Admissible, founded and complete alerts** (i.e. alerts that are managed by the Ethics & Compliance team) will be archived within **six months** after the end of the alert management and then deleted no later than **six years** after, in accordance with legal and regulatory obligations.
- **In case of judicial or disciplinary actions**, the alerts related data will be retained until the end of the relevant procedure, including applicable prescription periods, and then will be archived no more than **six years** to meet legal or regulatory obligations.

Speak Up tool Data Protection Statement

Privacy and Data Protection / Version 2.0 | 12.02.2025

Version	Date	Key Updates
1.0	01/02/2024	Creation
2.0	29/01/2025	Modifications on the overall statements
Modified by:	Data Protection Manager	
Approved by:	Group Data Protection Officer	

Introduction

This Speak Up whistleblowing alert tool ("Speak Up tool") Data Protection Statement ("Statement") sets out the general approach to dealing with the personal data collected from you or otherwise received by Pluxee International S.A.S. ("Pluxee") for the implementation and the management of the Speak Up, where it is stored, how it is protected and used, and who will have access to it and for what purposes. If there is any conflict between this Statement and the data protection laws in your country, then such laws, where applicable, will prevail.

What is the Speak Up tool?

The Speak Up tool is a voluntary, confidential web intake system operated by One Trust, an independent service provider, and provided by Pluxee to anyone who raises an alert as defined in the Speak Up whistleblowing Policy.

Access to the personal data processed through Speak Up is limited to Pluxee authorized persons on a need-to-know basis (e.g., users who are granted access for managing and investigating the reported alerts). Security and access rights are strictly managed in accordance with pre-defined user requirements. The system will limit user access to only the content and services to which the user is entitled.

Who operates the Speak Up tool?

Pluxee International S.A.S. (hereinafter designated as "Pluxee"), a company existing and organized under the laws of France, registered at the Registry of Commerce and Companies of Nanterre under the number RCS B 350 925 384 R.C.S. Nanterre, and located 16, rue du Passeur de Boulogne, 92120 Issy-les-Moulineaux in France acts as the Controller at a group level pursuant to its acceptance under French Data Protection Law.

What personal data is collected?

Pluxee collects and processes some limited personal data that may be shared by you such as: your name, your contact details, the name and other personal data of the persons you name in your report, and a description of the alleged misconduct as well as a description of the circumstances of the alleged incident.

Please be aware that the information you supply about yourself, your colleagues, or any aspect of Pluxee's operations may result in decisions that affect others. Therefore, Pluxee asks that you only provide information that, to the best of your knowledge, at the time when the information is provided, is correct, factual and useful for the investigation that will be undertaken. You will not be subject to disciplinary or adverse action by Pluxee for any report of a suspected legal or compliance violation that is made in "good faith", even if it later turns out to be incorrect. Acting in "good faith" means acting with an honest belief and intention. Please be aware that knowingly providing false or misleading information will not be tolerated.

Is it mandatory that I provide personal data to the Speak Up tool?

Use of the Speak Up tool is entirely voluntary. As a reminder, the normal route for reporting a possible violation is to escalate it to your manager or to a representative of the HR, Ethics and Compliance, or Legal Departments.

In the event that you are unable, or unwilling, to discuss such issues with your managers then the Speak Up tool has been set up to allow employees to report any irregularities or illegal actions witnessed or suspected, which may threaten to damage Pluxee's business or otherwise cause harm to the workplace.

Pluxee does not encourage anonymous reporting and in some countries, entirely anonymous alerts are not allowed. However, if requested, the alert to our service provider may be made on an anonymous basis, to preserve the identity of the individual(s) making the report, subject to local legal restrictions. Please review your local policy for further information.

How and for which purposes will the personal data collected be used?

Pluxee may process, use and disclose your personal data, for managing the Speak Up tool, for handling and, if necessary, investigating the alleged facts in your alert.

The alleged facts can be related to (i) a crime or an offense; (ii) a violation of or an attempt to conceal a violation of an international commitment regularly ratified or approved by France (iii) a violation of a unilateral act of an international organization taken on the basis of such an undertaking, European Union law, statute or regulation (iv) a violation of a law or a regulation; or (v) a threat of or serious damage to the public interest.

On which legal basis will my personal data be collected and processed?

Pluxee may have to collect and process your personal data where necessary for compliance with a legal obligation to which Pluxee is subject as well as Pluxee's legitimate interests (like for instance, legitimate interest in ensuring the health and security of its employees and the integrity, the reputation and the economic and financial health of Pluxee International) except where such interests are overridden by your interests or fundamental rights and freedoms.

To whom will the personal data be disclosed?

Your personal data will only be available to the persons, within Pluxee or external third parties, who need such access for the purposes listed above or where required by law.

The main categories of data recipients are the following (without this list being exhaustive): authorized internal users, third-party service providers or other contractors (with whom Pluxee has signed Data Processing Agreements) who process personal data on behalf of Pluxee and, as the case may be, judicial and regulatory authorities.

Different access levels are applied to data captured by the Speak Up tool to ensure that such data is visible only to appropriate users who need such access for the purposes listed above or where required by law.

The personal data will be disclosed and transferred to a third-party service provider which is involved in the provision of the Speak Up tool. This third-party service provider has been engaged under a binding confidentiality agreement with Pluxee International, whereby said third-party may act only upon the instructions of Pluxee International. Relevant personnel have been trained and authorized to manage and support the Speak Up tool.

This third-party service provider and/or other contractors, as the case may be, may be located in third countries (such as the United States), which data protection laws may not provide a level of protection equivalent to French data protection law.

If Pluxee discloses your personal data to such recipients, Pluxee will establish and/or confirm that, prior to receiving any of your personal data, they will provide an adequate level of protection for your personal data including appropriate technical and organizational security measures. In particular, if the recipients concerned are located in a country that does not provide an adequate level of protection (as this is the case in the United States), Pluxee will also rely on appropriate legal mechanisms, the relevant standard contractual clauses published by the European Commission, and the required supplementary measures to secure such transfer, in compliance with French data protection law.

How will my personal data be protected?

Pluxee implements appropriate technical and organizational measures to protect personal data against accidental or unlawful alteration or loss, or from unauthorized use, disclosure or access, in accordance with Pluxee's Group Information and Systems Security Policy.

Pluxee takes, when appropriate, all reasonable measures based on privacy by design and privacy by default principles to implement the necessary safeguards and protect the personal data processing. Pluxee also carries out, depending on the level of risk raised by the processing, a privacy impact assessment to adopt appropriate safeguards and ensure the protection of the personal data. Pluxee also provides additional security safeguards for data considered to be sensitive personal data.

What are my data protection rights and how can I exercise them?

You can consult at the following email address: <https://www.pluxeegroup.com/data-protection/>

How long will my personal data be held?

- ✖ **Inadmissible, unsubstantiated or incomplete alerts** (i.e. alerts that are not managed by the Ethics & Compliance team) are archived within a maximum of two months after their closure and then deleted not later than five years to meet legal or regulatory obligations.
- ✖ **Admissible substantiated and complete alerts** (i.e. alerts that will be managed by the Ethics & Compliance team) will be archived within six months after the end of the alert management and then deleted not later than six years to meet legal or regulatory obligations.
- ✖ **In case of judicial or disciplinary actions**, the alerts related data will be retained until the end of the relevant procedures, including applicable prescription periods and then will be archived not later than six years to meet legal or regulatory obligations.

How will I be notified if the uses of my data change?

If the use of your personal data in the Speak Up tool significantly changes, Pluxee will issue an updated Statement and/or take other steps to notify you beforehand of such changes so that you may review them and check whether they are acceptable (to the extent necessary) to you.

If you require further information about this Statement, please contact the Global Data Protection Office at the following email address: dpo@pluxeegroup.com.

If you require further information about the Speak Up tool, please contact your local System Administrator at speakup.group@pluxeegroup.com.

Who is my local system administrator?

If you should require any further information concerning this Statement and/or the Speak Up tool, please contact the department in charge of the helpline at speakup.group@pluxeegroup.com.



Thank you!