

Whistleblower Policy - Claranova Group



1 Introduction

- 1.1. This whistleblower policy (the “**Policy**”) is designed to establish a system within Claranova and its affiliates PlanetArt, Avanquest and myDevices, to enable personnel to report serious suspected wrongdoings within the Group and organize the collection and verification of all such reports.
- 1.2. Whistleblowers play an essential role in exposing fraud, corruption, unauthorized use of funds, mismanagement, criminal offenses, dangers to health and the environment and other wrongdoing that threatens integrity, both financially and morally.
- 1.3. This Policy is not intended to replace your employer’s regular information and reporting lines (notably through your HR department) but is intended as an additional mechanism for the reporting of suspected serious wrongdoing through a dedicated, secured, and confidential channel. This Policy does not replace any other specific complaints procedure already in place with your employer.
- 1.4. Claranova will implement this policy and procedure in its various jurisdictions and is entitled to amend this procedure when and where required.

2 Definitions

Alert: A report made by a Reporting Party whose purpose is to supply, via the External and Independent Whistleblower Platform, information pertaining to actions or behaviors deemed by the Reporting Party to be in breach of the applicable rules (see Paragraph 3.2 and 3.3 below).

External and Independent Whistleblower Platform: The dedicated external platform accessible from the Claranova website (<https://www.claranova.com>) and independent of Claranova 's information systems specifically designated by Claranova to collect Alerts and forward them to the Whistleblowing Committee, as specified in Paragraph 4.1 below.

3 Who may send an Alert, and what should it be based on?

- 3.1 The Policy is available to all employees and interns, and to all occasional and outsourced staff (collectively the **“Staff”**). It refers only to natural persons.
- 3.2 Any member of the **Staff** is therefore entitled to send an Alert (the **“Reporting Party”**), provided that the purpose of the Alert is to report one or more of the following:
- a crime or an offence;
 - a clear and serious breach of laws or regulations;
 - a serious and manifest violation of an international commitment regularly ratified or approved by your company’s country of origin;
 - a behavior or situations contrary to Claranova’s Code of Conduct concerning corruption and influence peddling; or
 - any threat or serious detriment to the corporate interest of any company of the Group,
- in which another member of Staff has participated (the **“Reported Individual”**).
- 3.3 However, Alerts should not include any information covered by the national defense secrecy, medical secrecy, or attorney-client privilege.
- 3.4 In any event, the Reporting Party must have personal knowledge of the facts or behaviors referred to in their Alert. He or she must act in good faith and selflessly.

Types of behavior that constitute grounds for an Alert

Definition	Examples
<p>Corruption</p> <p>Action by any individual consisting of illegitimately proposing, at any time, whether directly or indirectly, an offer, promise, gift, present, or any form of benefit to another person, for the latter or for any other person, as inducement for them to perform or refrain from performing any action that forms part of their job, mission, or mandate, or is facilitated thereby.</p> <p>The notion of corruption applies both:</p> <p>(i) to persons holding public authority, entrusted with a public service mission, or vested with elected public office; and</p> <p>(ii) persons who, without holding public authority, are neither entrusted with a public service mission nor vested with elected public office, exercise, during their professional or corporate duties, management duties or work for a natural person or legal entity or for any type of body whatsoever.</p> <p>‘Corruption’ may be active (proposing, offering, or promising), or passive (soliciting). Both behaviors are liable to prosecution.</p>	<ul style="list-style-type: none">• An employee offers an above-the-market discount to a distributor who pays a kickback to the employee.• Accepting a holiday offered by a supplier as a reward for an order.• Inviting the client and their spouse or partner to stay at a luxury resort to discuss an order.

<p>Influence-peddling Action by any individual consisting of illegitimately proposing, at any time, whether directly or indirectly, an offer, promise, gift, present, or any form of benefit to a person holding public authority, entrusted with a public-service mission, holding public elected office, for the latter or for any other person, as inducement for them to improperly use their actual or supposed influence for the purposes of securing distinctions, jobs, tenders, or any other favorable decision by an authority or a public administration.</p>	<ul style="list-style-type: none"> • Giving financial rewards to a public official for them to influence another person's decision in favor of Claranova.
<p>Moral harassment Moral harassment consists of repeated patterns of behavior against any member of Staff of which the purpose or outcome is a deterioration in the latter's working conditions liable to adversely affect their rights and/or dignity, lead to deterioration in their physical or mental health, or compromise their future career.</p>	<ul style="list-style-type: none"> • Humiliation • Denigration • Bullying and/or unfounded criticism • Oppressive measures • Aggressiveness • Isolation • Unjustified disciplinary pressure • Etc.
<p>Sexual harassment Constituted by repeatedly subjecting an individual to comments or behaviors with sexual connotations that are detrimental to the individual's dignity due to their degrading or humiliating nature, or creating an intimidating, hostile, or offensive situation for them.</p> <p>Any form of serious pressure, whether repeated or otherwise, exercised with the real or apparent aim of obtaining any act of a sexual nature, either for the benefit of the individual in question or for any other party, also constitutes sexual harassment.</p>	<ul style="list-style-type: none"> • Making comments to Staff about their private life and/or their anatomy, attempting to obtain sexual favors, and/or implementing professional measures as reprisals. • Sending erotic photographs. • Behavior that is insulting to a colleague, consisting of in sexually loaded insults and comments and/or inappropriate gestures. • Etc.
<p>Theft Fraudulent removal/appropriation of property belonging to another without their permission or consent.</p>	<ul style="list-style-type: none"> • Employees repeatedly and deliberately using the corporate bank card for purely personal purposes. • Knowingly participating in the removal of merchandise. • Etc.

4 **How to report an Alert**

- 4.1 The Alert can be submitted by the Reporting Party to their direct or indirect line manager, their employer, their staff representatives or to the members of the Whistleblowing Committee:
- the Group CEO;
 - the Chair of the Claranova Audit Committee;
 - the Group DPO.
- (together the "Whistleblowing Committee"), with the assistance of the Group Finance and Legal Department.**

By creating a written or audio report using the External and Independent Whistleblower Platform available via the Claranova website (<https://www.claranova.com>)

Upon receipt, the External and Independent Whistleblower Platform shall forward the Alert to the Whistleblowing Committee.

- 4.2 When submitting an Alert, the Reporting Party undertakes to abide by the technical security and confidentiality procedures defined by the Policy.
- 4.3 In the event of their computer momentarily being unused before the Alert has been finalized (e.g., non-finalized email), the Reporting Party undertakes to lock their computer session. If the Alert is submitted via the External and Independent Whistleblower Platform, the Reporting Party must ensure they are alone during the conversation with the latter.

5 Is there an obligation for the whistleblower to provide his or her identity?

- 5.1 In line with GDPR and other applicable data protection regulations, except in special circumstances where the Reporting Party believes it's crucial to remain anonymous, the Reporting Party is encouraged – thus not obligated in any way - to provide their name and contact details when submitting the Alert. This is to ensure the authenticity of the report and to prevent malicious or false allegations.

The identity of the Reporting Party will be processed and stored with the utmost confidentiality. It will not be disclosed to any individual, including the Reported Individual, unless required by legal or regulatory mandates. The Reporting Party has rights concerning their personal data under GDPR and other applicable data protection regulations, including being informed about its use and requesting its deletion. The data will be retained only for the duration necessary for the investigation and any subsequent legal or regulatory requirements.

6 What should be included in an Alert?

- 6.1 Any Alert must be worded in such a way as to be objective, relevant, and sufficient, and should be directly related to the scope of application of the Policy.
- 6.2 **Objective, Relevant, and Sufficient Information:** The GDPR emphasizes the principle of data minimization. Personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c)). Ensuring that alerts are objective and directly related to the scope ensures this principle is met.

Categories of Data:

Identity, position, and contact details: Considered personal data under GDPR. A legal basis is required for its processing. In the context of a whistleblowing system, the legal basis is the legitimate interests pursued by the organization (Article 6(1)(f)).

Facts reported: If these facts involve personal data, they too must be processed in line with GDPR principles. Ensure facts are relevant and not excessive. Not containing special categories of data (like racial or ethnic origin, political opinions, etc.).

Avoid Value Judgement or Subjective Comments: In line with GDPR's principles of accuracy (Article 5(1)(d)) and data minimization (Article 5(1)(c)). Personal data should be accurate.

- 6.3 No value judgement or subjective comment on individuals' behavior shall be taken into account; no such information should be included in the Alert.
- 6.4 The Alert may be supported by information and documents in any form or medium.

7 Who receives and processes the Alert?

- 7.1 The Whistleblowing Committee receive and process all Alerts. They assess that any Alert submitted to them falls within the scope of application set forth in Section 3, and that processing is a legal obligation for Claranova or presents a legitimate interest, or if it can be dismissed.
- 7.2 If the Alert processing is confirmed, the Whistleblowing Committee can investigate the facts, either themselves or by entrusting this task to a restricted number of individuals acting under their supervision, notably HR personnel or external advisors.
- 7.3 Based on the observations made during this verification, the Whistleblowing Committee shall decide, in concertation with the relevant Human Resources department, whether disciplinary, judicial, or administrative proceedings should be brought against the Reported Individual.
- 7.4 The implementation of any disciplinary proceedings against the Reported Individual and/or any other person whose liability may have been found to be engaged during verification of the facts, shall take place in accordance with the provisions of your company rules.

8 Guiding principles to process the alerts

- 8.1 All investigations should be carried out in a fair and transparent manner, without unreasonable delay, and in accordance with all regulations.
- 8.2 The following principle should be applied to all investigation, irrespective of the level of risk posed by the alleged facts reported in the Alert:
 - Absence of retaliation: The Reporting Party and people who cooperate with the investigation must be protected against retaliation, whether during the investigation or after its conclusion, for their cooperation.
 - Confidentiality: Investigations must be conducted with the strictest confidentiality, including allowing access to the information related to the investigation only on a need-to-know basis.
 - Competence: Team investigating the report should be made up of people adequately skilled to understand the issues at stake when carrying out the investigation.
 - Independence: An investigation must be conducted only by those who do not have an interest – or an appearance of interest – in the matter they are investigating.
 - Objectivity: All information gathered during an investigation must be reviewed and analyzed according to the same standards, and the findings of an investigation should be based upon facts. Investigations shall be free from personal opinions and bias.
 - Timeliness: Investigations should be conducted in a timely manner to ensure that wrongly accused people are cleared and ongoing wrongdoing is stopped as quickly as possible.
 - Thoroughness: All facts related to a specific situation must be thoroughly analyzed, including by reviewing the documentation and interviewing the relevant persons.

9 Investigation process

- 9.1 The Whistleblowing Committee will evaluate the nature and complexity of the issues raised through the Alerts. They will evaluate the context of the allegation as well as any possible implications for the Group and the person accused of wrongdoing. Based on their preliminary observations, they should plan out the overall timeline and schedule of the investigation.
- 9.2 The Whistleblowing Committee and/or the entrusted individuals should consider whether there are any related ongoing or prior investigations that may aid the current investigation.
- 9.3 The Whistleblowing Committee and/or the entrusted individuals should also consider whether there are immediate actions that should be recommended to (i) prevent imminent injury or harm to people or property or to avoid any continued non-compliance, or (ii) prevent

destruction of any relevant documentation or information necessary for the investigation.

- 9.4 The Whistleblowing Committee will involve in the internal investigation those individuals who they deem to be the most competent in the subject and impartial. In doing so, the Whistleblowing Committee will refer to the content of the Alert and the nature of the allegation in determining who should be part of the investigation team. If the Whistleblowing Committee determine that the content of the Alert requires technical knowledge in a specific industry, they may assign an industry specialist to their team.
- 9.5 The Whistleblowing Committee and/or the entrusted individuals should draft an investigation plan, and should focus on the following issues:
- What information is necessary to the investigation;
 - Who the potential sources of information may be and whether they should be interviewed;
 - What, if any, internal policies and procedures are contravened in the alleged misconduct or wrongdoing;
 - Whether the Reporting Party could be interviewed;
 - Which documents and/or other evidence will be used during the course of interviews, and which documents and/or evidence will be requested during said interviews; and
 - The specific issues to be covered during an interview.
- 9.6 As part of the investigation plan, the Whistleblowing Committee should contemplate which information should be communicated and to whom, and how such communication will be managed.

10 Data retention methods and duration

- 10.1 To ensure transparency and accuracy, while respecting the rights of data subjects under the General Data Protection Regulation (GDPR), the Whistleblowing Committee is limited to processing the following categories of data:
- **Reporting Party's Details:** This includes their identity, position, and contact details.
 - **Reported Individual's Details:** This includes their identity, position, and contact details.
 - **Details of Relevant Personnel:** This pertains to the identity, position, and contact details of all individuals actively involved in the reception and subsequent processing of the Alert.
 - **Reported Facts:** Precise, objective details about the incident or concern raised.
 - **Verification Information:** Data acquired or consulted during the verification process of the reported facts.
 - **Verification Summary:** A concise report or summary detailing the process and outcome of the verification conducted.
 - **Alert Follow-up:** Any additional actions, communications, or resolutions arising post-verification of the Alert.

In all instances, data retention will align with GDPR principles, ensuring data is held only as long as necessary to fulfill the purpose of the whistleblowing policy, after which it will be securely deleted or anonymized. It is crucial that periodic reviews are conducted to ascertain that all retained data remains pertinent and is not held beyond the necessary duration.

- 10.2 It is reminded that employees must identify the private nature of their messages exchanged and / or stored on the networks by carrying the mention "private" or "personal" in their subject

line and to classify them as soon as they are sent in a file itself called "private" or "personal". All messages not identified as "private" or "personal" are deemed professionals and the property of the employer. As such, professional messages can be accessed by the employer.

- 10.3 If, following receipt by the Whistleblowing Committee, the data pertaining to any given Alert is deemed not to fall within the scope of this Policy, it shall be destroyed or stored forthwith, subject to application of Section 12.
- 10.4 Consistent with the General Data Protection Regulation (GDPR), any data related to Alerts that have undergone verification will be either deleted or archived within two months from the completion date of the verification process. Exceptions to this rule apply in instances where disciplinary, judicial, or administrative actions are initiated against the Reported Individual or, in cases of malicious Alerts, against the Reporting Party.
- 10.5 If a disciplinary procedure or legal proceedings are brought against the Reported Individual (or the Reporting Party in the event of a malicious Alert), the data concerning the Alert shall be stored pursuant to legislation in force until the completion of the proceedings in question.
- 10.6 Data subject to data archiving shall be stored within a distinct, restricted-access information system, for a duration not exceeding the maximum periods for legal proceedings set forth in the applicable law.
- 10.7 The Whistleblowing Committee and the External and Independent Whistleblower Platform shall take all appropriate precautions to preserve the data security during gathering, communication, and preservation thereof. They shall ensure that data is not distorted, damaged or become accessible to unauthorized third parties.
- 10.8 In this respect, access to the processed data shall entail compliance with specific established authentication procedures. Furthermore, all such access shall be logged, and the appropriate nature and compliance thereof controlled by the Whistleblowing Committee.

In instances where data processed pursuant to the Alert are transferred outside of the European Union, such transfers will be in strict compliance with the General Data Protection Regulation (GDPR) provisions related to international data transfers, the relevant stipulations of the French Data Protection Act (Loi Informatique et Libertés), particularly Articles 68 and 69, and will be subject to the Standard Contractual Clauses as adopted by the European Commission.

The execution of this Policy requires the processing of personal data. Accordingly, it has been drafted in line with the stipulations set out in the General Data Protection Regulation (GDPR). Moreover, it adheres to the terms laid down in Decision no. 2017-191 of the French Data Protection Agency (CNIL) dated June 22, 2017, amending Decision no. 2005-305 of December 8, 2005. This grants a Single Authorization for the automated processing of personal data within the framework of whistleblowing systems (AU-004), in conjunction with the guidance issued by the CNIL on July 18, 2019.

11 Rights of the Reported Individual

- 11.1 Once an Alert has been recorded, computerized or in any other format, the Whistleblowing Committee shall advise the Reported Individual of the personal data concerning them that is being processed, the allegations, and, unless when anonymity is required, the identity of the person(s) processing the Alert.
- 11.2 In no event shall the Reported Individual be informed prior to the Whistleblowing Committee having taken any necessary precautionary measures, particularly with a view to preventing the

destruction of evidence vital to dealing with the Alert.

- 11.3 The Reported Individual shall have a right to access the data concerning them, on request to the Whistleblowing Committee. In no event may this right of access extend to information concerning third parties, and more particularly, the identity of the Reporting Party.
- 11.4 Furthermore, the Reported Individual may request modification of incorrect, incomplete, ambiguous, or obsolete data concerning them.
- 11.5 However, the Reported Individual may not exercise any right to rectify data concerning them before the time required for the Whistleblowing Committee to process the Alert has elapsed.

12 Rights of the Reporting Party

- 12.1 Any Reporting Party who is subject to inappropriate behavior or retaliatory measures due to an Alert having been raised pursuant to this Policy must advise the Whistleblowing Committee *via* the External and Independent Whistleblower Platform. The Whistleblowing Committee shall take all appropriate measures to protect them in such circumstances.
- 12.2 Perpetrators of inappropriate behavior or retaliatory measures shall be liable for disciplinary, judicial, or administrative sanctions pursuant to its employer's rules and applicable laws and regulations.
- 12.3 The Reporting Party shall have a right of access to data concerning them and may exercise this right on request by sending an email to the Whistleblowing Committee thru the Whistleblower Platform.
- 12.4 Furthermore, the Reporting Party may request rectification of incorrect, incomplete, ambiguous, or obsolete data concerning them, on request, by sending an email to the Whistleblowing Committee thru the Whistleblower Platform.
- 12.5 The Reporting Party must be promptly informed that the Whistleblowing Committee have received their Alert, which shall specify the reasonable period they anticipate will be required to verify the admissibility of the Alert and how they will advise the Reporting Party of the action taken as a result. All such communication shall take place *via* the External and Independent Whistleblower Platform.
- 12.6 Raising an Alert in good faith shall not entail any disciplinary sanctions against the Reporting Party, even if the allegations are incomplete or prove to be incorrect.
- 12.7 However, any Reporting Party triggering an Alert in bad faith, for instance by deliberately supplying false or incorrect information, or with malicious intent, shall be liable for disciplinary sanctions.