Alleima

Alleima Way

Speak Up procedure

PP - 05409 – v.2.0

1 Purpose

This document outlines the procedures to follow when undertaking an investigation[1] into a reported or suspected breach of the Code of Conduct, Alleima Policies and/or the Law, notified through the Speak Up reporting system, or through another source such as an Internal Audit report or reported to and/or by management. Non-investigation related reviews or procedures do not fall within the scope of this procedure, e.g., Performing a follow up on a customer complaint relating to service quality. Similarly, grievance related issues that are followed up in accordance with existing HR procedures are excluded from the scope of this procedure, however these reviews should be performed in accordance with the relevant HR grievance procedure and formalized accordingly.

The document is to be read in conjunction with the Alleima Ethics & Compliance Policy under which this procedure is authorized.

[1] Defined as "the act of examining something carefully, especially to discover the truth about it" (Cambridge dictionary)

2 Definition(s)

2.1 Privacy in relation to an investigation

Reports of alleged breaches of the Code of Conduct in almost every case have an impact on specific individuals and employees. As such, the matters raised can have direct bearing on the reputations, careers and future livelihoods of those persons. Maintaining their right to privacy and justice while dealing with any reported breach is a central principle of this procedure. Privacy principles applicable to the country concerned must be considered and appropriate steps taken to comply with relevant legislation applicable to that country. These considerations apply in each of three phases of the investigation and the subsequent remediation process.

The privacy of the reporter is likewise central to the integrity of the reporting system. Reports must be treated with strictest confidentiality, with the privacy of both the reporter and implicated person/s preserved while the matter is investigated. Sensitive information is kept strictly confidential with the "need to know" principle, both regarding information and persons involved.

An additional consideration is the privacy aspects of accessing employee data from the company IT systems. This needs to be done in a manner compliant with relevant data privacy regulations and company practice. In terms of preserving sources of data such as personal computers, telephones, and email/OneDrive files, this needs to be facilitated through an appropriately approved data preservation request issued to and facilitated by IT Security with the process for reviewing the data appropriately supported, overseen by Business Integrity and approved by the Group General Counsel and/or Group Head of Compliance. Depending on the circumstances, it may be appropriate to appoint a competent consultant company to support the review and host the data on a review platform. For this reason, any requirement to preserve sources of data and/or conduct email and document reviews in support of an investigation must be managed through the procedures established together with IT Security, with advice from Business Integrity, as required.

2.2 Confidentiality

2.2.1 Who to inform

A fundamental principle of all investigations is the application of the ‘need to know’ principle:

- Only those persons who have a need to be informed of the investigation, shall have knowledge of the case.
- The basis of a person’s needs to know must be assessed prior to providing information about the case, usually because the person:
  - will support the investigation;
  - will carry out the remediation;
  - will provide oversight of the investigation;
  - is accountable for the operations of the business and/or may be responsible for a possible legal liability for the business; or
  - is responsible for managing external communication on cases that may have substantial impact on the company share price or overall reputation.

2.2.2 When to inform

Alleima conducts investigations to discover whether or not a breach has taken place, but the purpose of an investigation is also to uncover the facts so that corrective actions can be taken. Therefore, the person/s who will remediate the problem should be brought into the investigation process as early as possible.

2.3 Presumption of innocence

The presumption of innocence is the legal principle that one is considered innocent until proven guilty. In many countries, presumption of innocence is a legal right of the accused in a criminal trial, and it is an international human right under the UN's Universal Declaration of Human Rights, Article 11.

Although the company’s investigation process cannot be compared to a trial, and the purpose of an investigation is to obtain the facts, this principle should be kept in mind and the individual performing the investigation should identify and report on the facts, remaining impartial and unbiased throughout the process and not taking side (actual or perceived) in the matter under investigation.

2.4 Escalation – Conflict of Interest

When assessing who can be involved in an investigation, persons possibly implicated or conflicted by the report must be thoroughly considered throughout the course of the investigation and resultant remediation process.

An individual that may be implicated or conflicted in a Speak Up report or concern, or may be perceived to be conflicted, cannot oversee, or carry out the investigation. The case must be escalated to someone who is not, or does not appear to be, conflicted. This is to ensure that no conflict of interest arises in which an implicated or conflicted person oversees or can otherwise influence the direction of an investigation, possibly in favor of their own interest.

If a potential conflict of interest situation arises in the course of the investigation that implicates a person already involved in the conduct of the investigation, Alleima Speak Up Intake Committee (Head of Business Integrity, General Counsel, VP HR and Head of Compliance) must be consulted to agree the measures to be taken, for example removing the conflicted person from all or parts of the investigation.

Similarly, the seniority of the subject of the investigation is a key factor to consider and in particular in respect of the impartiality and independence of the investigation process. The Alleima Speak Up Intake Committee must consider the appropriateness of those on the envisaged investigation team in relation to the subject of the investigation.

Investigations in relation to any member of the GEM should be overseen by the General Counsel (or if conflicted, the Chief Executive Officer or Chairman of the Audit Committee).

2.5 Document retention

2.5.1 Retention

A case file must be retained, and the case must be updated in the Speak-up system. Investigations initiated from other sources, such as concerns communicated to management or issues and allegations received from sources other than the Speak Up reporting mechanism, should be recorded in the Speak-up system or alternatively tracked in terms of progress, outcome and resultant remediation actions taken. Recording of, and updates relating to, the matter must be done timely throughout the investigation and remediation process to reflect the status of the investigation and actions taken.

In addition to Personal Data included in the original Speak Up report or any other source of information to the investigation, information obtained during the investigation typically includes various types of Personal Data which must be safeguarded by the investigator responsible for the investigation and subsequently deleted/purged, as explained below.

2.5.2 Deletion

Deletion of Personal Data contained in the Speak-up system is done by the investigator in accordance with the Statute of Limitations for the country concerned or other jurisdiction/s that may have an interest in the matter. The investigator may store certain investigation records on his/her company issued computer, however these records must be purged when no further legitimate interests exist.

Sensitive Personal Data retained in any case file maintained on Speak-Up or any other system (company issued computers, physical papers, emails, case management system, Teams, etc.) must be deleted, per the below rules:

If the investigation confirms that no breach of the Code of Conduct or a law has taken place, the case is classified as "Unsubstantiated"– The deletion of all personal identifiable information must be done when no further legitimate interests exist.

If the investigation confirms that a breach of the Code of Conduct or a law has taken place, the case is classified as "Substantiated" - For the purpose of protecting Alleima against potential litigation, all substantiated cases shall be stored for as long as the relevant retention period allows, typically the Statute of Limitations for the relevant jurisdiction, or any other jurisdiction that may have an interest in the matter. The purpose of the storage is to keep a record of all original case details, which may include personal information about the reporter and eventual implicated parties, in case of future claims. Upon closing a substantiated case, the access to it shall be greatly restricted to limit the number of persons with access to any personal information logged within the case.

3 Scope

Breaches of the Alleima Code of Conduct, Policies and/or Law may pose risks to Alleima's reputation and can result in financial and other losses (e.g. reputational). Alleima is committed to fair play and with our ambition for continuous improvement, implementing appropriate corrective action is key both to sustainable and reliable compliance programs as well as to prevent recurrence. As such, when an alleged breach or concern is notified, whether through the Speak Up reporting system or by other means, it is important that the breach is investigated promptly. If the claims of a breach are substantiated, where the investigation performed establishes that the breach is in fact confirmed, then Alleima is responsible for initiating remedial action to address the breach. This may involve implementing changes in procedures and controls, instituting appropriate disciplinary action, reporting to relevant authorities or other appropriate actions such as terminating a contract with an external party involved in the breach. These corrective actions, typically referred to as remediation, are taken to deal with the impact of the breach and reduce the risk of a similar breach in the future.

4 Procedure

4.1 The Investigation 'life-cycle'

The overall process or 'life cycle' is a three-phase process from the initiation of a case at the beginning, to closing out a case at the end, summarized as follows:

4.2 Case initiation, 'triage' & planning

All investigations start with a catalyst an event or an incident that is reported. The report may originate from someone who has called or used the online interface of the Speak Up reporting system. It may also originate from someone who has referred a concern directly to their manager, HR or to a Compliance Officer or Legal Counsel. In addition to these sources, Internal Audit findings and Business Integrity investigation findings may pose new issues for investigation.

Whatever the catalyst, this procedure starts from the point at which the reported alleged breach of conduct is reported directly to management or entered into the Speak Up System.

Once the incident is reported, a 'Triage' and risk assessment is performed from the information available to assess the severity of the 'injury' or prevalent risks. The Triage assessment is performed by the Alleima Speak Up Intake Committee (Group; General Counsel, VP HR, Head of Compliance and Head of Business Integrity).

Before commencing the investigation, it is important that the planned investigation steps be documented, and the objective of the investigation be understood and clearly stated so as to provide direction as to what the investigator sets out to achieve. If the matter is referred to appropriate managers, a hand over call together with a detailed referral to Management document is handed over from the Business Integrity function.

The Investigation Planning performed taking the following into consideration:

- What it is you have to investigate?
- When did the alleged incident occur and what period of time needs to be included?
- Where did it occur?
- Who was involved in the reported incident?
- Is there any available evidence (e.g., witnesses, documentations, videos, photos, messages etc.)?
- Are there any potential conflicts of interest?
- How will you perform the investigation?
- Why specific resources (for example, the data, documents or preservation of the data) are needed and is there a need to involve external legal counsel (the General Counsel should involve external counsel when considered necessary)
- Whether there are any reporting obligations to authorities or regulators (the General Counsel and/or external legal counsel should advise as appropriate)
- Assess potential implications for Alleima as a Group where very serious matters should be escalated/ alerted to the appropriate level as soon as possible to allow control of the risk and oversight of the process

The plan should be reviewed and approved by the relevant Responsible Parties, normally in discussion within the Speak Up Intake Committee.

4.3 The Investigation process

An investigation seeks to establish the facts relevant to substantiating the allegations. These may be sourced from:

- Witnesses;
- Individuals with direct and/or relevant knowledge or information e.g. a finance manager or business controller; and
- Electronic and hard copy records from the relevant department.

The collection of information should be appropriately documented, recording the date, time and source of the information received by the investigation.

Preserving and accessing an individual's data may be subject to specific laws and regulations within the jurisdiction the individual and data are located. As such, there are specific steps and checks that must be undertaken to ensure compliance with all relevant laws and regulations and by way of example, a separate legitimate interest assessment may need to be prepared in accordance with local data privacy legislation for the relevant jurisdiction.

In terms of preserving sources of data such as personal computers, telephones, and email/OneDrive files, this needs to be facilitated through an appropriately approved data preservation request issued to and facilitated by IT Security with the process for reviewing the data appropriately supported, overseen by the Head of Business Integrity and approved by the Group General Counsel and/or Group Head of Compliance. Depending on the circumstances, it may be appropriate to appoint a competent consultant company to support the review and host the data on a review platform. For this reason, any requirement to preserve sources of data and/or conduct email and document reviews in support of an investigation must be managed through the procedures established together with IT Security, with advice from Business Integrity, as required.

It is these facts, appropriately supported with confirming evidence in the form of witness statements or interviews and information sourced from electronic and/or hard copy records, which are documented in an investigation report, that allow management to make appropriate decisions and lead to the implementation of appropriate remediation steps.

4.4 Remediation

Remediation comprises the following phases:

Risk assessment and planning - The planning landscape for remediation starts with the areas identified in the investigation report for corrective action and is based on a root cause analysis in establishing what failed. These can include a range of internal actions such as appropriate disciplinary action, re- training of personnel, revision of relevant steering documents, changes in controls, audit and resources to name a few. They can also include a range of external actions such as legal actions against third parties and the possibility of requiring disclosure to authorities, which would have already been considered in the planning phase of the investigation. The weight of evidence in support of each proposed corrective action will be a factor in populating the risk assessment. Another factor that may constrain the possible remedial course of action is what is permissible or not under local law.

Implementation – Execution of the planned remediation steps. (normally performed by appropriate management)

Closure – Finalization of the investigation and remediation providing evidence that Alleima has dealt with the identified breach comprehensively in a risk-based manner. This is an important pillar to the overall Compliance program of the Group.

Actions taken to remediate a breach of the Code of Conduct may not be risk free. Before implementing a proposed remediation action, the remediation manager should consult with the relevant line managers,

Business Integrity and in cases with severe impact for Alleima the Speak Up Intake Committee should review associated risks and agree through approval before the remedial actions are executed.

4.5 Timing

In order to ensure an appropriate level of confidence in the process, investigation matters must be performed timeously. The following timeframes apply to all investigation matters[2]:

- Acknowledgement of receipt of the report from the reporting person – **7 days of receipt**
- Finalization of the investigation and providing feedback[3] to the reporter – **period not exceeding 3 months** (as an exception, highly complex matters may extend beyond this period but must be closely monitored by the appropriate Approving Party).

[2] In accordance with 'The EU Directive for the protection of persons who report breaches of Union law' ("Whistleblower Protection Directive")

[3] Defined in the Whistleblower Protection Directive as providing information on the action envisaged or taken following the investigation.

5 Roles and responsibilities

Roles and responsibilities apply at a Group, and Divisional level, as follows:

Group:
Head of Business Integrity provides regular summary reports to the Group Audit Committee, Group General Counsel as well as the respective Group VP HR representatives with updated extracts reflecting the status of reports received through the Speak Up reporting mechanism and/or other matters recorded in the system. Business Integrity provides further oversight of investigation matters initiated through Speak Up, follow up on the status of matters, draws statistics in accordance with predefined targets and ensures implementation of this Procedure. Business Integrity also provides oversight and technical support in relation to investigation matters.
Speak Up Intake Committee (General Counsel, VP HR, Head of Compliance & Head of Business Integrity) must consider the appropriateness of those on the envisaged investigation team in relation to the subject of the investigation. In addition, responsible for the Triage (prioritization) and risk assessment and in cases with severe impact for Alleima the Speak Up Intake Committee should review associated risks and agree through approval before the remedial actions are executed.

Division:
When appointed by the Speak Up Committee as co-investigator or main investigator are responsible for executing the investigation according to this procedure.

Responsibility for each investigation is determined by issue type, as follows:

Overall responsibility: Group General Counsel	Group VP HR
Functional oversight: Head of Group Compliance / Head of Business Integrity	Group VP HR / Divisional HR
Issue type: - Bribery - Kickbacks - Extortion - Conflict of interest - Nepotism and Cronyism - Fraud - Embezzlement - Communication matters - Inaccuracy of records - Tax matters - Unauthorized use or disclosure - Theft - Business Critical Information - Trade Controls - Supplier Conduct - Unfair competition - Competition law & anti-trust issues	- Freedom of Association and Collective Bargaining - Child Labor - Forced or Compulsory labor - Health and Safety - Working Hours - Retaliation - Equal Opportunity - Discrimination - Harassment - Sexual Harassment - Pollution - Waste - Chemicals - Personal Information

6 Performance management

- Compliance to EU Whistleblowing Directive
- Compliance to Global data privacy requirements

7 References

- Alleima Ethics & Compliance Policy

8 Appendix

N/A