StrongPoint Whistleblowing Channel Policy & Procedure

StrongPoint will not tolerate any form of misconduct or critical conditions, such as violations of statutory rules, internal rules, policies or ethical standards, such as bullying, harassment, discrimination, corruption, money laundering or any other financial fraud, and will make efforts to ensure a safe, healthy and legal environment in all our business activities and legal units.

Breaches of any local and/or EU/EEA law may result in disciplinary actions, including termination / dismissal and reports to the relevant authorities.

The StrongPoint Whistleblowing Channel is a tool enabling anonymous submission of any suspected breach of the local and/or EU/EEA law from both inside StrongPoint and outside. It fosters confidential communication between reporter and case handler.

StrongPoint Whistleblowing is compliant with the EU Whistleblower Directive (Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law) and the regulations regarding whistleblowing in the WEA (local working environment and protection laws).

Objective

The objective of this procedure is to describe the handling of cases submitted to the StrongPoint Whistleblowing Channel, according to the EU Directive, local legislation and the internal procedures while at all times ensuring the protection of the Notifier.

The output of this process is that the reported case is handled with discretion and closed, with necessary actions taken.

This procedure is owned by StrongPoint Chief People and Organization Officer and was last updated in November 2023.

Definitions

Case handler - the Whistleblowing Country Manager or other assigned personnel who will handle the report.

Intake Management (IM) - a service established using Microsoft Forms which receives the reports and assigns cases within one business day based on a predefined schema.

Notifier - is a person who reports a breach of EU/EEA or local law. They can be any employee, former or existing, or self-employed person in StrongPoint, a shareholder, or someone from outside of StrongPoint, e.g third persons connected with the Notifier or StrongPoint's suppliers and customers who need to notify of a breach or a potential breach of the local or EU/EEA legislation or any of StrongPoint's internal rules/policies.

Report - the reported whistleblowing case.

Viewer - a case handler with temporary and limited access to the report, requested by the case handler.

MS Forms - the chosen tool for handling whistleblowing reports.

Whistleblowing Manager (WM) - a StrongPoint employee, typically from Management, HR, Legal or Finance, responsible for coordinating and managing whistleblowing for all the StrongPoint companies in their assigned country.

Who can report?

This procedure applies to a Notifier who needs to report a breach or a potential breach of the local or EU/EEA law or any of StrongPoint's internal rules/policies, such as StrongPoint's Code of Conduct.

It also applies to third persons who are connected with the Notifier, and who could suffer retaliation in a work-related context, such as colleagues or relatives of the Notifier.

As a Notifier, you are protected by law. You should not be treated unfairly or lose your job because you 'blow the whistle'.

What can be reported?

All reports shall be based on justifiable grounds of suspicion. Evidence is not necessary, but reporting must not be made with the intention to cause harm or with the knowledge that the accusation is false. Hence, the report you disclose must be made in the public interest. To identify if a report is in the public interest, you should look at the following criteria:

- the number of people affected

- the nature or impact of the harm
- who is the reported individual.

In a nutshell, the report should go beyond the employee's personal circumstances.

Some examples include the following:

- a criminal offense, for example, fraud
- someone's health and safety are in danger
- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law – for example, it does not have the right insurance
- you believe someone is covering up wrongdoing
- #MeToo cases

Whistleblowing that fulfils this criteria shall be treated as a "Qualified Reporting" and handled in accordance with the StrongPoint Whistleblowing Procedure.

What cannot be reported?

Types of cases other than those listed above should not be reported. Such cases that do not fulfil the criteria will be treated as "Non-qualified reporting". A non-qualified reporting will not be handled within the StrongPoint Whistleblowing Procedure.

Examples of cases that should not be reported through the StrongPoint Whistleblowing Channel are:

- General opinions on how the business is run
- General opinions on salary, leadership or other personnel matters

Such cases shall be handled by reporting to the relevant manager or any other relevant person within the management of the company in question.

This is the standard response the Notifier will receive in case of a "non-qualified reporting":

> Thank you again for your report.
>
> After a careful review, we do not consider this to be a whistleblowing matter and will close the case. Our recommendation is to speak with your closest manager or contact HR/other.
>
> Please note that you will not be able to respond to this message. Should you not be happy with how your case was managed you are welcome to submit a new one.
>
> Kind regards,
>
> STRONGPOINT Whistleblowing

Where the reporting should be done

Reporting shall be made using:

https://www.strongpoint.com/strongpoint-whistleblower-channel/

which is the only and official online StrongPoint Whistleblowing Channel.

Reporting is made by submitting a form either anonymously or with a full name. Providing your full name might in some cases increase the chance of resolving the reported case, however, it is fully the Notifier's decision to disclose their identity or not.

If you are reporting anonymously please make sure that you put down as much information about the matter as possible and at least the following:

- The StrongPoint company connected with the misconduct/breach of local/EU/EEA law
- Description of the misconduct/breach and who's involved
- Facts, evidence or proof of the misconduct/breach

Other channels:

As a Notifier you can come to our StrongPoint office and ask to see the *Whistleblowing Country Manager (WCM).* A list of offices and address you can find on: https://www.strongpoint.com/contact/.

As a Notifier you can connect to the management of StrongPoint. A list of management representatives you can find on: https://www.strongpoint.com/investor/corporate-governance/executive-management/.

Contact the **Chief People and Organization officer at phone number: +47 40010888.**

Note! If an alert is received through a different channel than the official online one, the recipient shall use the StrongPoint Whistleblowing Channel to register the case or contact the relevant Whistleblowing Country Manager. The same steps shall be used in handling the case.

The whistleblowing process and its actors

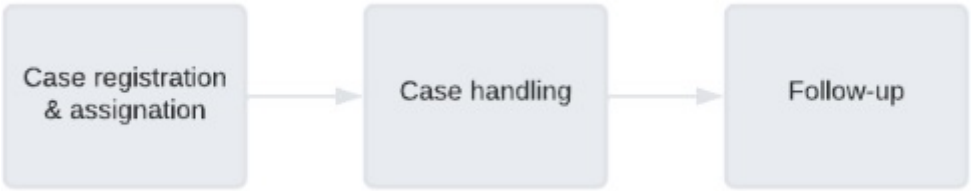

Figure 1. Whistleblowing case handling process overview

Report registration and case handler assignation

When StrongPoint receives a report submitted through the Whistleblowing Channel, the Intake Management (IM) will immediately receive a notification for channeling the alert to the designated Whistleblowing Managers which are always two people either from Management, HR or Finance.

StrongPoint uses this set-up also to ensure impartiality and transparency.

Each country will have two Whistleblowing Managers assigned for backup reasons which include vacation or any type of leave, or if one of them is mentioned in the report, then IM will assign the case to the other one.

Once the case is assigned to the main Whistleblowing Manager, the Notifier will receive an acknowledgement of receipt.

The standard automatic response which will be sent to the Notifier is this one:

> Thank you for submitting your concerns. We hereby confirm that we have received your case and we will review it carefully.
> All future communications from us will be sent via the channel established in your report.
>
> Best regards,
>
> STRONGPOINT’s Whistleblowing

Whistleblowing case handling

The provision in Article 8(3) of the EU Directive 2019/1937 specifies that each StrongPoint company with 50 or more workers is required to set up channels and procedures for internal reporting, where such legal entities belong to a group of companies.

Article 8(6) allows medium-sized companies to share resources as regards the receipt of reports and any investigation to be carried out. It should be underlined that the responsibility to maintain confidentiality, give feedback, and address the reported breach remains, however, with each medium-sized company concerned. Only medium-sized companies can benefit from this possibility, and companies that belong to the same group.

The Whistleblowing Country Managers have the responsibility to create local procedures for internal reporting, while the local channels are facilitated through case handler assignation.

All cases reported through the official Whistleblowing Channel will be tracked through logs.

Qualified or Non-Qualified report

The case handlers on the platform, i.e. the Whistleblowing Managers or the relevant personnel assigned to handle the case, will need to decide as per procedure and local legislation whether the report is to be treated as Qualified or Non-Qualified report.

If the case handler decides that it is a Non-Qualified report, the report can be immediately closed by sending a standardized communication to the Notifier and exclude it from statistics.

> Thank you again for your report.
>
> After a careful review, we do not consider this to be a whistleblowing matter and will close the case. Our recommendation is to speak with your closest manager or contact HR/other.
>
> Please note that you will not be able to respond to this message. Should you not be happy with how your case was managed you are welcome to submit a new one.
>
> Kind regards,
>
> STRONGPOINT's Whistleblowing Function

If the report is considered to be Qualified, the relevant case handlers are obliged to start the investigation process. The report will be marked as a "Whistleblowing case" and will count in the statistics.

Case handling per company size

For StrongPoint companies the Whistleblowing Managers will forward the report to the Board of Directors chairman in these legal units and to the Group Chief People and Organization officer.

For this reason, one of the fields in the report that should be filled in is "Please select the StrongPoint company this report pertains to." It should be made clear that this information is

important so their case is better handled by the relevant people and in accordance with the EU directive.

Best practices for case handling

If the Notifier decides to submit the case by presenting their identity they should be invited to a meeting or a call to discuss the content of the report and to provide more background information regarding the relationship and/or discussion of further handling of the case. In this meeting, clarifications and agreements shall be made on how to communicate in the further course of the case, including consideration to immediately inform the relevant StrongPoint Company's Board and/or the StrongPoint Group Board.

If the report is submitted anonymously through the whistleblowing channel, the Whistleblowing Managers will coordinate the best course of action for handling the case, depending on the specifics of the reported issue.

To collect more information, the Whistleblowing Managers or any other assigned case handler on the case, can and are encouraged to contact the notified in confidentiality using the contact details provided, and store the correspondence securely for further reference.

Important to remember:

- Involve external assistance depending on the degree of impartiality and persons involved (e.g. the management)
- The method should be adapted to the nature of the problem, the content and the persons involved. Methods that *may* be used:
    - Document analysis
    - Conversations
    - Use of experts
    - Consultation with immediate contradiction (gather both parties in one room, when possible - get the facts on the table)
    - Interviews with key persons that may have information regarding the suspicion or the case
- Review of documents, e.g. accounting, project implementation.
- Keep the Notifier informed - they need to receive at least one follow-up notice within 90 days
- When the Notifier discloses their identity, their manager shall ensure that any retaliation is prevented
- If at any point the Whistleblowing Manager or the case handlers encounter whistleblowing reports including but not limited to reputational damage, litigation, financial risk, etc. they should involve StrongPoint’s Group Crisis Team by contacting the , for support.
- Ensure the wellbeing of the Notifier by providing them:
    - Legal aid (when appropriate)
    - Health care (if necessary)
    - Leave of absence (when necessary)

Follow-up

As per the requirements of the EU Directive, the main case handler who can be the Whistleblowing Manager or assigned personnel, needs to provide follow-up communication to the Notifier within 90 days since the report was submitted, even if the case is not concluded within that time frame.

Depending on the severity, the Whistleblowing Manager or relevant Board of Directors will consider contacting the local National Authority for Investigation and Prosecution of Economic and Environmental Crime.

Appropriate measures should be taken (mitigation or/and prevention regarding future similar cases).

Documentation requirements

All activities related to the case must be documented. Necessary documentation must be gathered by the case handlers or the Board of the StrongPoint company (when applicable) who shall document everything during the process. At the closing of the case a copy should be provided to the Chief People and Organization officer in StrongPoint.

All documentation shall be stored in a secured location (restricted OneDrive or similar). Tracking or log of all follow-ups in relation to a report should be saved (e.g. document added, messages sent, etc.).

Personnel data will be processed in accordance with the StrongPoint Privacy Statement.

User access and management on MS Forms reporting tool

For safety reasons, there are only two users that have elevated rights: the Administrator (Chief People Officer) and one backup administrator among the Whistleblowing Managers.

Revisions of policy and version log

Request of policy changes or updates can be shared with the owner of this policy, StrongPoint People and Organization Officer.

Version 2.1 (20.11.2023) – Major policy revision and updates implemented. Replaces the policy amended in the CoC.

Version 2.1.1 (12.12.2023) – Updated online version and MS Forms tested.