

Policy and Guidelines for Whistleblower Protection Framework

Table of Contents

Background.....	3
Purpose	3
Framework for the Protection System	3
What can be Reported?.....	3
How is Misconduct Reported?	4
How are Reports Processed?.....	4
Notifying Persons Involved	5
Data Processing	5
Unfounded Reports	5
Follow-Up and Audit	5
Publication	6
Information	6

Background

In 2018, cBrain established cBrain's Code of Conduct (CoC). Any deviations from the CoC must be reported to the CFO, who will then report to the Board of Directors.

As a result of the company's growth, recommendations from the Corporate Governance Committee, and the EU's approval of the directive requiring listed companies to implement a whistleblower protection framework, cBrain decided to establish a whistleblower protection system, effective from the 10th of May 2021.

Purpose

The purpose of the protection framework is to ensure anonymity of individuals who report breaches as outlined in the section "What can be reported?".

These guidelines outline the scope of the whistleblower protection system, including its uses, how it functions, how data is processed, how to inform the relevant parties, and contact details for further inquiries, among other details.

By doing so, these guidelines ensure that all users will be able to understand and properly execute the procedure.

Framework for the Protection System

The whistleblower protection framework can be used by individuals associated with the company - such as employees, management, Board of Directors, suppliers, customers, advisors, or others connected to the company - who wish to report serious misconduct or suspected serious misconduct, see the section "What can be reported?".

Other types of misconduct or inappropriate behavior not covered by the framework should be reported through the usual channels.

What can be Reported?

cBrain encourages the reporting of any serious misconduct, either through the company's usual channels or via the whistleblower protection framework. The whistleblower framework serves as an alternative and supplementary reporting channel.

Misconduct includes:

- Financial crime
- Violations of relevant stock exchange rules, auditing rules, and accounting rules
- Fraud
- Forgery
- Corruption
- Theft
- Security breaches in IT systems
- Violation of GDPR rules
- Pollution
- Health and safety violations
- Violation of the cBrain's Code of Conduct (<https://cbrain.com/s/Code-of-conduct-engelsk.pdf>)
- Violation of legislation

The term "serious misconduct" refers to situations

- which can cause serious harm to people and society.
- which are considered illegal.
- which may result in reprimands from authorities or auditors.
- which may damage the company's reputation and relationships with employees, customers, or the outside world.

How is Misconduct Reported?

Serious misconduct can be reported via the "Report" hyperlink, which is available on the company's website. This link provides access to the external and independent service "EQS Integrity Line".

EQS Integrity Line ensures whistleblower's anonymity and guarantees that their identity cannot be traced by cBrain.

While it is encouraged to include one's name in the report to facilitate and streamline the investigation process, reports may also be submitted anonymously.

The following must be stated in the report:

- The informant's relation to the company
- Time and date/period of the misconduct
- Description of the misconduct
- Any persons involved
- Adverse effects of misconduct

How are Reports Processed?

Reports are submitted to the Chairman of the Audit Committee.

If the report concerns the Chairman of the Audit Committee, the Chairman of the Board of Directors will assume responsibility for handling the matter.

If the report concerns the Chairman of the Board of Directors, cBrain's external auditor, PwC, will be entrusted with the task.

All reports will be thoroughly investigated unless clearly unfounded.

Where necessary and appropriate, the Chairman of the Audit Committee or the Chairman of the Board of Direction may seek internal or external assistance to investigate the matter.

All individuals involved in the investigation are required to maintain strict confidentiality.

Every report will result in a written statement containing a conclusion and/or recommendation.

The conclusion/recommendation can be:

- Closed/unfounded
- Closed/procedure modified
- Closed/reprimand given
- Closed/disciplinary action taken
- Closed/the case should be reported to the police
- Closed/the case should be reported to the authorities

The statement will be submitted to the Board of Directors.

In case of a particularly serious matter, the Board of Directions may be notified during the investigation.

Notifying Persons Involved

Once a preliminary investigation has been conducted, the person or persons named in the report must be notified without delay. The notification must include information about the person responsible for the investigation, the nature of the report, and who has access to the resulting statement. The identity of the information will not be disclosed unless required by law.

As the person named in the report, you have the right to access the contents of the report. However, you are not entitled to any information that could reveal the identity of the informant.

If the report is shown to be unfounded, you have the right to be informed of the informant's identity.

If you believe that any information in the report is incorrect, misleading, or incomplete, you have the right to request a correction. If cBrain is unable to accommodate the request, your comments will be recorded as supplementary information in the report.

Data Processing

Data related to any reports or investigations is stored and processed in accordance with applicable legislation as described below.

Reports and related documentation are stored by EQS. EQS ensures that only authorized users can access the data and that data is stored with the necessary precautions. cBrain has entered into a data processing agreement with EQS.

Data will be deleted immediately after a case is handed over to the authorities or the police. In cases involving disciplinary actions or reprimands, relevant information will be stored in the employee's personnel file. Information concerning employees will be deleted at the end of the third year following termination of employment.

Reports determined to be unfounded will be retained for the current year plus one additional year after the case is closed, in order to monitor for repeated unfounded allegations.

Reports determined to be outside the scope of the whistleblower framework will be forwarded to the appropriate person in cBrain's management. These reports will also be stored for the current year plus one additional year after the case is processed, to monitor for repeated out-of-scope issues.

Unfounded Reports

An employee who reports misconduct in good faith – even if the report is later found to be unfounded – will not face any consequences.

However, deliberately false reports will not be tolerated. If made by an employee, such actions may lead to disciplinary consequences, including potential termination of employment. Deliberately false reports from external parties may be referred to the appropriate sanctioning authorities.

Follow-Up and Audit

The Audit Committee will annually review the nature and development of any reports and inform the Board of Directors accordingly. In addition, the Audit Committee will also reassess the procedure each year and update it if necessary.

Publication

The procedure can be accessed through the company's website.

Information

If you have any questions concerning the whistleblower protection framework, you can contact Ejvind Jørgensen, CFO by e-mail ejj@cbrain.com or by phone +45 2594 4973.

Log

Version	Date	Author	Description
1.0	2021.02.23	EJJ	Document created. Approved by the Audit Committee. Approved by the board of directors
1.1	2021.03.26	EJJ	Added handling of unfounded reports or reports out of scope. Approved by the board of directors.
1.2	2021.04.28	EJJ	SOP and Guidelines have been combined into one document – "Policy and Guidelines" to avoid repetition. Approved by CFO
1.3	2025.08.12	EJJ	Minor linguistic corrections made. Approved by CFO