

**Policy and Guidelines for Whistleblower Protection Framework**

Table of Contents

[Background 3](#_Toc70525516)

[Purpose 3](#_Toc70525517)

[Framework for the Protection System 3](#_Toc70525518)

[What can be Reported? 3](#_Toc70525519)

[How is Misconduct Reported? 4](#_Toc70525520)

[How are Reports Processed? 4](#_Toc70525521)

[Notifying Persons Involved 5](#_Toc70525522)

[Data Processing 5](#_Toc70525523)

[Unfounded Reports 5](#_Toc70525524)

[Follow-Up and Audit 5](#_Toc70525525)

[Publication 6](#_Toc70525526)

[Information 6](#_Toc70525527)

## Background

In 2018, cBrain established a Code of Conduct. Deviations from the CoC must be reported to the CFO, who will subsequently 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 establish a whistleblower protection framework, cBrain has decided to implement a whistleblower protection system from the 10th of May 2021.

## Purpose

The purpose of the protection framework is to ensure anonymity of persons who report breaches described in the section “What can be reported?”.

These guidelines describe what the whistleblower protection system can be used for, how the system works, how data is processed, how to inform persons involved, contact person for further questions etc.

Thereby, these guidelines will ensure that any user will be able to understand and execute the procedure.

## Framework for the Protection System

The whistleblower protection framework can be utilized by persons associated with the company such as employees, management, Board of Directors, suppliers, customers, advisors, or others connected to the company, who could wish to report serious misconduct or suspicion of serious misconduct, see the section “What can be reported?”.

Other unregulated behavior must be reported through the usual mediums.

## What can be Reported?

cBrain encourages that any serious misconduct be reported to the company either through the company’s usual mediums or through the whistleblower protection framework. Thus, the whistleblower protection framework is an alternative and supplementary medium.

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 company’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 persons 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 hyperlink “report”, which can be found on the company’s website. From there, one can gain access to the external and independent service “EQS Integrity Line”.

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

It is encouraged to state one’s name in the report to aid and simplify the process of investigating the misconduct. Certainly, one may also submit a report 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 the misconduct

## How are Reports Processed?

Reports are submitted to the Chairman of the Audit Committee.

If the report involves the Chairman of the Audit Committee, the Chairman of the Board of Directors will be entrusted with the task.

If the report involves 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.

To the extent necessary and required, the Chairman of the Audit Committee/the Chairman of the Board of Direction may request internal and external help to uncover the situation.

Those involved in the investigation are required to maintain full confidentiality.

All reports will result in a written statement which contains a conclusion/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

When a preliminary investigation has taken place, the person or persons involved in the report must be notified without delay. The notification must include information on the person in charge of investigation, the nature of the report, and who has access to the statement being prepared. No information is provided concerning the identity of the informant, unless required by law.

As someone involved in the report, you have the right to gain access to the report. However, you do not have the right to any information concerning 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 concerning the misconduct is either incorrect, misleading, insufficient, etc., you have the right to request that the information be corrected. If cBrain is unable to comply with the request, the information will be referred to as supplementary information in the report.

## Data Processing

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

EQS stores reports and statements. EQS ensures that only authorized users may access 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 has been handed over to the authorities or the police. In cases involving disciplinary action or reprimands, related information will be stored on the employee’s personnel case. Information concerning employees will be deleted at the end of the third year after termination of employment.

Reports shown to be unfounded will be stored for the ongoing year + 1 more year after the case has been processed to monitor whether there are repeatedly reported unfounded misconduct.

Reports shown to be out of scope will be forwarded to the right person in cBrain’s management. Afterwards, the report will be stored for the ongoing year + 1 more year after the case has been processed to monitor whether there are repeatedly reported misconduct out of scope.

## Unfounded Reports

An employee who in good faith reports misconduct, which is subsequently shown to be unfounded, will not face any charges.

Deliberate false reports will not be tolerated. If done by an employee, it can have consequences for employment. Deliberate false reports from outsiders will be submitted to sanctioning body.

## Follow-Up and Audit

On a yearly basis, the Audit Committee will follow up on the development and character of any report(s) and will subsequently inform the Board of Directors. Furthermore, the Audit Committee will also reevaluate the procedure on a yearly basis and update the procedure if deemed 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 by e-mail ejj@cbrain.com or by phone +45 2594 4973.