CYBERNETICA

Public

Procedure for the Reporting of Breaches of European Union Law and Unethical Behaviour

29.10.2026

P-167-20

© 2026 Cybernetica AS

Table of Contents

1 Purpose 3

2 Roles 4

3 Scope 5

3.1 Areas in which breaches may occur 5

3.2 Examples of breaches may include 5

4 Reporting breaches 7

5 Rights and responsibilities of reporting person 9

6 Confidentiality 10

7 Protection and non-retaliation 11

1 Purpose

This document outlines the legal basis for reporting breaches of European Union law and unethical behaviour that are discovered in the course of work, as well as the protection of persons who report such breaches in accordance with the Act on Protection of Persons Who Report Work-Related Breaches of European Union Law.

Cybernetica is committed to compliance with applicable laws and regulations and maintaining high standards of business ethics and corporate governance.

The purpose of the document is to define Cybernetica's general rules and commitment to handling breaches, protecting reporting persons, and provide an overview of how a breach can be reported.

Cybernetica expects all employees and third parties to report concerns related to Cybernetica's activity. Compliance with this document is mandatory for all employees and third parties when reporting breaches.

The legislation of the Republic of Estonia and/or the European Union shall prevail over the statements of this document and adjustments can be done to comply with the legislation of the Republic of Estonia and/or the European Union. These adjustments must be made with subsequent versions of this document.

This document shall be updated once every five (5) years or as needed to reflect changes in applicable legislation.

2 Roles

The following roles are involved in the handling of breach reports as appropriate:

- Cybernetica employee – reporting person internal to the company (e.g. intern, person working under an employment contract or contract of service);
- Third party – reporting persons external to the company (e.g. job applicant, employee with whom the employment relationship has ended);
- Human Resources Manager – owner of the document who remains responsible for the adequacy of this document and renewal, if necessary;
- Council – a three-member council, the members of which are a human resources employee, a working environment specialist and a quality manager appointed by the board's decision, who process violation reports;
- Management Board – the highest management body to which a member of the council regularly provides non-personalized reviews of breach reports and which makes the necessary management decisions;
- Lawyer – General Counsel or Legal Counsel to be involved in the management of a breach report when it comes to legal matters;
- Project manager – person to be involved in the management of a breach report if the breach report relates to a specific project;
- Process manager – person to be involved in the management of a breach report if the breach report relates to the management of processes or documents;
- Head of Department – person to be involved in the management of a breach report if explanations are needed regarding matters relating to intern department matters;
- External proceeding of the complaint – person to be involved in the management of a breach report if its involvement is mandatory or necessary under the law (e.g. Data Protection Inspectorate, Police and Border Guard Board, Estonian Internal Security Service).

3 Scope

Reporting of breach refers to a situation where an employee or a third person (hereinafter referred to as “reporting person”) reports an incident related to a breach involving Cybernetica.

Examples of possible areas in which violations may occur and of the violations themselves are given in the following points but these examples are not comprehensive and primarily have an informative meaning in the context of Cybernetica's field of activity.

3.1 Areas in which breaches may occur

- public procurement;
- prevention of money laundering and terrorist financing;
- product safety and compliance;
- environmental protection;
- privacy for personal life and personal data protection;
- network and information security.

3.2 Examples of breaches may include

- criminal offences or breaches of other legal or regulatory requirements, failure to observe a legal obligation, corrupt or fraudulent behaviour (e.g., economic offence, fraud etc.);
- unethical behaviour (e.g., making inappropriate comments at work-related events, harassment etc.);
- breaches of contract (e.g., knowledgeable breach of a client contract etc.);
- careless use and/or misappropriation of Cyberneticas property (e.g., unsupervised use of Cyberneticas property in public, etc.);
- putting people’s health and safety at risk (e.g., non-compliance with work organisation rules etc.);
- financial and non-financial administrative malpractice (e.g., not observing proper procedures etc.);
- fraud or deliberate error in the preparation, evaluation, review or audit of financial accounts and records (e.g., conscious processing of false information, deliberately providing inadequate information etc.);

- participation in or condoning a reportable wrongdoing through wilful suppression or concealment of any information relating to a wrongdoing (e.g., failure to report harassment cases etc.);
- non-compliance with environmental, social responsibility or governance framework (e.g., improper sorting of garbage etc.);
- personal grievances by employees or third parties. Personal grievance is a concern, problem or complaint that is specifically related to the person (e.g., bullying by co-workers, unfair treatment by direct manager, dissatisfaction with the terms and conditions of employment contract, etc.).

For the avoidance of doubt, the examples provided under clauses 3.1 and 3.2 do not contain the exhaustive list of breaches and are provided for informational purposes only.

4 Reporting breaches

Reports of breaches must be submitted to the address whistleblowing@cyber.ee which is managed by the human resources employee appointed by the board's decision or his/her substitute.

For the avoidance of doubt, Cybernetica requires reporting persons to report in Estonian or in English. Any report made in another language might need further translation and council cannot guarantee the same level of judgement as there remains possibility of information being misinterpreted through translation.

Although the reporting person is not required to furnish any more information than what he/she wishes to disclose, it is essential for Cybernetica to have all critical information in order to be able to effectively evaluate and investigate the allegation. The report should provide as much detail and be as specific as possible, including names and dates, in order to facilitate the investigation.

To the extent possible, the disclosure by the reporting person must include the following:

- type of concern (what happened);
- when it happened (date or a period of time);
- where it happened (office, department);
- the name(s) of the employee(s) and/or external party(ies) involved in the breach;
- witness(es), if he/she/they are available;
- some proof of allegations, if possible;
- who can be contacted for further information;
- expectations when processing a breach report (desired outcome).

Reports of breaches are received and analysed by the human resources employee appointed by the board's decision or his/her substitute who must record and store every report in full details alongside the decision taken on the report and the reasoning thereof. Reports of breaches must be reviewed immediately, but not later than within seven (7) days after receipt.

In case the reporting person has a reason to distrust the human resources employee appointed by the decision of the board or his/her substitute, the reporting person is allowed to send a breach report to the human resources manager, e-mail head-hr@cyber.ee, whereas the human resources manager will then take the full responsibility of handling the report with the instructions and requirements established in this document.

The human resources employee appointed by the decision of the board, his/her substitute or the human resources manager has the right to address the report to the council. If the investigation has been taken to this stage, the aforementioned make sure that the identity of the reporting persons shall remain confidential and information regarding the report shall be forwarded to the council in the manner maintaining confidentiality and keeping any other information related to the reporting person as minimal as possible.

In case a report is made against the member of the council, the human resources employee appointed by the decision of the board, his/her substitute or the human resources manager have the responsibility to exclude the member of the council in question (including him/herself) from the council and to continue with the council in a reduced state or form a new council in such a way that it does not include the person against whom the report is made. Only those

persons who can be considered the most suitable to handle the report in question are entitled to be included in the council. Under no circumstances can the name of the reporting person be reported to the removed member of the council (except in a situation where the member of the council is forced to remove himself).

A member of the council is obliged to provide the management board with an overview of the reports that have been submitted during that quarter once a quarter. Such overview shall be conducted in a manner enabling the reporting persons to maintain their confidentiality. It shall be highly emphasized that the management board has the right to such information that does not put the reporting persons in any way or form at a disadvantage.

5 Rights and responsibilities of reporting person

All breach reports must be made in good faith and with a reasonable belief that the information in the notice is true.

If the reporting person submits a report of breach in good faith and reasonably believing it to be true, but it is not confirmed by the investigation, Cybernetica will recognise the concern, and no negative consequences will follow. If, however, the reporting persons make an allegation frivolously, maliciously or for personal gain, legal consequences may follow.

Reporting persons may be contacted for further information by the person responsible for handling the report of breach, except in a situation where the person clearly forbids it.

Reporting persons must provide sufficient corroborating information to justify the commencement of an investigation. All reports will be taken seriously and investigated as fully as possible, but without sufficient information, it may be more difficult to evaluate the credibility of the allegations and, therefore, less likely to cause an investigation to be initiated.

Reporting persons are "reporting parties", not investigators. They are not to act on their own in conducting any investigative activities, nor do they have a right to participate in any investigative activities other than as requested by the person handling the case.

If, when handling the report of breach, it becomes clear that it is necessary to communicate with the competent authorities (such as but not limited to Police and Border Guard Board), then the person responsible for handling the report of breach ensures that during the investigation of the report, the circumstances and evidence of the case are recorded with accuracy that is sufficient for further investigation of the report and satisfies the requirements of the investigative authorities.

Reporting persons are informed about the status of their report and, if possible, also the steps that Cybernetica has taken to investigate the facts of the report, unless legal requirements or Cybernetica’s reasonable interests prohibit disclosure of status of the investigations. Such feedback shall be submitted to the reporting persons as soon as possible, but no later than three (3) months or, in justified cases, six (6) months after receiving the report.

All reports of breaches are subject to a legal retention obligation, which is three (3) years from the moment the investigation has been ended and feedback given to the persons who report work-related breach.

6 Confidentiality

All information received will be treated with confidence, except where Cybernetica is required by law or regulation to disclose it, for legal or audit purposes or where Cybernetica refers the matter to relevant authorities.

The protection of a reporting person's identity will be maintained to the extent possible within the legitimate needs of law and the investigation. Cybernetica will make every effort to keep the identity of the reporting persons confidential. However, there may be circumstances where, due to the nature of the investigation, it will be necessary to disclose the reporting person's identity.

In order not to jeopardise the investigation, the reporting person is also required to keep confidential the fact that a report has been made, the nature of the breach and the identities of those involved, unless required to disclose such information by law or regulation.

7 Protection and non-retaliation

Cybernetica is committed to the fair treatment of all persons submitting genuine and appropriate reports of breaches, including the protection of reporting persons against unfair dismissal, victimisation, or unwarranted disciplinary action. Reasonable steps will be taken by Cybernetica to protect the reporting persons from reprisal or inconvenience as a result of making a report of breach.

It is a breach of this document for any Cybernetica´s employee or third party to cause inconvenience to a reporting person who submits any report under this policy in good faith and reasonably believing it to be true.

A reporting person shall immediately report any alleged or apparent retaliation to the Human Resources Manager. Cybernetica will promptly investigate claims of retaliation and changes in employment that might constitute retaliation against any employee or third party who has engaged in any of the protected activities. Cybernetica reserves the right to take appropriate action against any person who initiates or threatens to initiate retaliation against reporting persons who make reports of breach under this document.

A reporting person’s right to protection from retaliation under the corresponding state laws does not extend immunity for any complicity in the matters that are the subject of the allegations or an ensuing investigation.