WHISTLEBLOWER AND COMPLAINT POLICY

COMPUTER 2000

Revision 01
May 2023

WHISTLEBLOWER AND COMPLAINT POLICY

Table of Contents

Why it is important

COMPUTER 2000 Bulgaria (the Company) is committed to the highest standards of integrity, openness, and accountability. Protecting our reputation requires continuous and rigorous attention to possible incidents of misconduct involving suspected fraud, corruption, collusion and coercion, and other serious infringements of the rules and policies in force at the Company. We welcome and take seriously feedback from anyone working with us.

The purpose of this policy is to ensure all employees, contractors and external parties understand how to report incidents such as misconduct or illegal practices in good faith, without having to fear that such an action may have adverse consequences for the whistleblower.

This policy applies to all current, former and potential employees, contractors, interns and other external parties who may have witnessed misconduct or illegal behaviour on behalf of the Company.

What to report

The types of acts of misconduct that can be reported under these guidelines are broadly categorised, but not limited to:

- Misconduct that constitutes a criminal offence directed against the Company's interests, and in particular fraud, corruption, or misconduct regarding accounting regulations;
- Human rights or environment-related risks, as well as violations of human rights or environmental obligations that have arisen as a result of the Company's business activities;
- Workplace misconduct such as workplace harassment, sexual harassment, intimidation, and conflict of interest;
- Misconduct that violates anti-discrimination laws;
- Other misconduct that violates the Company's Code of Conduct or other rules and policies.

How to report

Content of the report. Reporting misconduct should be made in good faith. In order to enable the Company to investigate the reported incident or risk properly and effectively, the report should be based on facts and answer questions such as:

- What happened where and when?

- Who was involved?
- Can a repeat of the incident be expected? If so, when and where?
- Who else could have knowledge of the incident or access to the information about it?
- Are there any documents related to or evidence of the incident described?
- Is there any additional information that could possibly be relevant and helpful?

Employees, business partners, and other third parties can confidentially report information regarding the risks and violations. They may opt for anonymous or not anonymous reporting. In the case of not anonymous reporting, the Company will take all necessary measures to keep confidentiality and prevent any form of retaliation.

Reporting can be done through the following channels:

- by e-mail to: compliance@computer2000.bg
- by regular mail addressed or delivered to: COMPUTER 2000 Bulgaria, Compliance officer, 63, Shipchenski prohod Blvd. Sofia 1574, Bulgaria

What happens next

The whistleblower report is handled by the Compliance Officer. The first step in the procedure is to determine whether there are grounds for a more detailed investigation, and if so what types of expertise is required. The information and evidence provided by the whistleblower will be the basis for the investigation. This step may result in two decisions:

- If the report is not based on facts and the allegations cannot be verified, the Compliance Officer will close the case.
- If the report is deemed to be valid and admissible, the Compliance Officer will initiate a detailed investigation.

A detailed investigation will include the collection and analysis of documentary, video, audio, photographic, and electronic information or other material, interviews of witnesses, observations of investigators, and other investigative techniques that may help to conduct the investigation. The investigation will be conducted in a fair and unbiased manner and the implicated staff member will be given a fair hearing.

If additional expertise is required, the Compliance Officer may set up a committee to investigate the report, ensuring that the committee does not involve persons against whom the whistleblower report is filed. Further external parties might be involved, such as legal authorities, depending on the nature of the complaint submitted. Alternatively, the

Compliance Officer may decide to investigate the case personally, if setting up a committee may compromise the anonymity and objectivity of the inquiry.

The investigation results are documented in accordance with legal requirements. The Compliance Officer determines the grievance of the misconduct and related risks and is responsible for taking appropriate countermeasures. In some cases, complaints may be resolved internally – for example through the dismissal of an employee, cancellation of a contract with an external service provider, etc. In other cases, complaints might need to be submitted to the responsible law enforcement authorities.

The whistleblower has the right to be notified of any action taken regarding their complaint, with due care to the safety and security of the reporting person.

Protection against retaliation

All whistleblowers reporting suspicions of misconduct or illegal practices in good faith will be protected from any retribution or adverse consequences. This refers also to employees who report anonymously and might be subsequently identified.

The Company is committed to protecting whistleblowers against retaliation from an affected party in the event that the whistleblower's identity is known or suspected.

False reporting

This Policy is not aimed at encouraging malicious and false allegations and should not be used for such reporting. Allegations that are known to be false and not made in good faith are an abuse of this Policy.

"Good faith" herewith means the unequivocal belief in the veracity of the reported misconduct, i.e., the fact that the whistleblower reasonably believes the transmitted information to be true.

Employees who make a report in bad faith, particularly if it is based knowingly on false or misleading information shall be treated as a breach of the loyalty and professional ethics requirements of the Code of Conduct.