Group Speak Up Policy

Raising concerns at work; Computacenter's Speak Up (Whistleblowing) Policy

Who does this policy apply to?

Everyone working with Computacenter or any subsidiary company of this Group; this includes all employees and temporary workers employed through a third party and its strategic partners ("Computacenter"). The reporting process within this policy is also open to anyone working with Computacenter as part of our supply chain.

This policy will be updated from time to time, so please ensure that if you are an employee you refer to the OneCC Compliance pages*, or for non-employees, refer to Computacenter's corporate website to make sure you are accessing the current versions of this policy.

If you are a manager or hold a senior position, you have an obligation to understand what the risks could be within your area of operation and to take immediate action if you believe there is a risk to Computacenter. This means it's essential that you know what your reporting obligations are if you are approached with a report directly.

This means all managers and those in a senior position need to familiarise themselves with this policy and the "Guidance for Managers" document that provides helpful advice and supports you in meeting your obligations when a concern is raised with you directly.

Why do we have this policy?

Our customers and our people trust in us to be an ethical, compliant, and sustainable organisation. Computacenter is committed to observing high ethical standards in the conduct of its business activities and complying with the laws that apply across our countries of operation.

We believe it's important for you to speak up about any concerns you have at work. This is known as whistleblowing. This policy explains what to do if you have a concern or you suspect something you've seen or heard about is unsafe, unethical, unlawful, or not in line with our company policies and/or the interests of others or of Computacenter itself (or anything else that you reasonably believe would be in the public interest).

We understand that you may feel worried about raising a concern, but rest assured, it's safe for you to speak up without the fear of retaliation. We will ensure that any reporting details are kept in strictest confidence and that you are able to report any concerns anonymously.

What's meant by 'Public Interest'?

This is where the interests of others or of Computacenter itself are at risk, such as:

- Criminal offences
- Bribery and corruption
- Breaking the law

- Miscarriage of justice
- Danger to health and safety
- Damage to the environment
- Deliberately hiding information about any of the above.

Raising Concerns

You have an obligation to speak up if you have any suspicions of inappropriate conduct so that it can be investigated as soon as possible. Don't wait until something goes wrong before acting. There will be no negative consequences for any concerns raised with reasonable belief and made in good faith even if they turn out to be unfounded.

The earlier you raise a concern, the easier it is for us to act. You don't need to have firm evidence before you tell us, but you'll need to explain what's happened to cause you to have a concern about a situation, and if you have any thoughts on how we can resolve the issue.

Whichever way you raise a concern, whether it's by telling your line manager, informing another appropriate contact in the Computacenter Group, or through Safecall's external and confidential whistleblowing hotline you can be sure that your concerns will be taken seriously.

Any person who raises a concern will not be subject to any detriment, retaliation, discrimination, or other adverse consequences. Retaliation against any individual for raising a legitimate concern is not tolerated by Computacenter. Such retaliation is an extremely serious breach of both company policy and law and may lead to action under local disciplinary policies or / and labour laws up to and including dismissal.

If your concern is about your employment with Computacenter, you can speak to either a manager of your choice or a member of your in-country HR team who will be able to explain how you can raise a concern.

Third-Party Reporting line: Safecall

Our people are strongly encouraged to report any concerns around potential violation of any Computacenter policy to the independent, confidential hotline supplied by Safecall.

Safecall provides an independent, confidential reporting line where you can raise your concerns. Calls are handled by skilled staff and treated in complete confidence.

Once a report has been raised, this is passed to the Director of Group Legal and Compliance and the Chief People Officer to establish the right course of investigation. If the report relates to either of these, then the report is instead passed to the Company Secretary.

The regional leads of compliance may be included in an investigation, providing the report does not relate to their area of responsibility. All reports are treated on a strictly confidential, need to know basis.

You can contact Safecall 24 hours a day, seven days a week. The phone number to call is dependent on the country you're calling from.

Safecall can also be contacted by email on computacenter@safecall.co.uk or via the web at www.safecall.co.uk/report.

Country	Telephone Number (all free of charge)
Australia	1 800 312 928
Belgium	00 800 72332255
Canada	1877 599 8073
China	4008 833 405
France	00 800 72332255
Germany	00 800 72332255
Hong Kong	3077 5524
Hungary	00 800 72332255
India	000 800 4401256
Ireland	1800 812740
Japan	0120 921 067
Malaysia	1800 220 054
Mexico	800 1231758
Netherlands	00 800 72332255
Poland	00 800 72332255
Romania	0372 741 942
Singapore	800 448 1773
South Africa	0800 990243
Spain	00 800 72332255
Switzerland	00 800 72332255
UK	0800 9151571
USA	1866 901 3295

If you are contacting Safecall from a country not listed above, you can find a full list of the phone numbers by country on the following link: Telephone Numbers (safecall.co.uk)

What happens if I raise a concern?

Once a concern has been raised (whether via Safecall or another means) the individual receiving the report or made aware of the allegations (in cases where it is not directly raised to Safecall) has an obligation to treat any information received and the identity of the reporting person in complete confidence.

If the report is not received in the first instance via Safecall, the person who is made aware of the allegations should log it with Safecall or report it directly to the Group Legal and Compliance Director or the Chief People Officer. The concern should not be discussed with anybody outside of this to ensure that confidentiality is maintained.

In receipt of a report, the Director of Group Legal and Compliance or Chief People Officer will make sure that an independent and impartial review of the matter is conducted without delay, taking all measures necessary to resolve or correct the matter.

In the event that a report relates to suspected criminal activity information will be reported to the local authorities, as appropriate.

Will I find out what happens if I raise a concern?

We'll let you know where possible the progress of any investigation, but this may not always be possible because of the confidentiality required for each concern reported.

*For our people based in China or Hong Kong this Policy and supporting documents will be provided to you via an email communication. You can also request a copy from your Line Manager

Annex 1: WHISTLEBLOWING POLICY IN COMPUTACENTER POLAND Sp. z o.o. (hereinafter: COMPUTACENTER)

1. Why is it important to report suspected violations?

COMPUTACENTER conducts business with integrity and expects all associates to act in accordance with the law and internal standards and policies. Building an ethical and friendly working environment is a priority for us. We realise how important it is to report potential irregularities and encourage everyone to report suspected violations. Thanks to reporting, **COMPUTACENTER** can react faster and prevent incidents that could carry any risks to people and the workplace.

This document is the local internal reporting policy (whistleblowing policy), in compliance with the Act on the Protection of Whistleblowers dated June 14, 2024. In addition to the internal reporting policy (hereinafter: the Policy), **COMPUTACENTER** also adopted group regulations such as: *Group Speak Up Policy, Group Speak Up Process* under which reports of suspected violations may be made under the terms described therein.
In the event that the provisions of the global regulations would conflict with the Policy or would be irreconcilable with the provisions of the Policy or national laws, only the Policy shall apply.

2. What can be reported?

The policy applies to reports of all cases of violation and circumvention of the law, concerning:

1. corruption;
2. public procurement;
3. financial services, products and markets;
4. anti-money laundering and countering the financing of terrorism;
5. product safety and compliance;
6. transport safety;
7. environmental protection
8. radiological protection and nuclear safety; ;
9. food and feed safety
10. animal health and welfare;
11. public health
12. consumer protection;
13. protection of privacy and personal data
14. security of networks and information and communication systems;
15. the financial interests of the State Treasury of the Republic of Poland, a local government unit and the European Union;
16. the internal market of the European Union, including public law principles of competition and state
17. constitutional freedoms and rights of a human being and a citizen - occurring in the relations of an individual with public authorities and not related to the areas indicated in point 2. 1-16,

(hereinafter: the **Report**).

3. Who can report?

The Report can be made by all persons who have become aware of the violation in a work-related context, in particular: employees, former employees, job candidates, representatives of **COMPUTACENTER**, persons employed under civil law contracts, management contracts, or providing services or goods to **COMPUTACENTER** under other contracts (hereinafter: the **Whistleblower**).

4. How to report?

The Report may be submitted via the Safecall platform, in writing or verbally, to computacenter@safecall.co.uk; via the website www.safecall.co.uk/report to the phone number: 00 800 72332255 or during a face to face meeting with the HR Manager at COMPUTACENTER of the Polish entity. The face-to-face meeting to can be requested through the Safecall whistleblowing platform as detailed above and will be arranged within 14 days of such a request.

The Report can also be made anonymously.

5. What information should be included in the Report?

The Report should include a description of the violation, the circumstances under which the violation occurred (or may occur), information useful to clarify the case (including details of persons who were involved in the violation or may help explain the circumstances of the violation, the place where the violation occurred, and when the violation occurred). The Whistleblower may indicate in the Report the preferred method of communication regarding the Report.

6. Who receives the Report?

All reports, regardless of how they are submitted, go to the HR manager (hereinafter: **the Receiving Entity**).

The Receiving Entity within 7 days of obtaining the Report shall acknowledge its receipt to the Whistleblower, unless the Whistleblower has not provided a contact address.

7. Who investigates the Report?

The entity that assesses, verifies reports and conducts follow-up actions is the Investigating team (hereinafter: the Investigating team). The Investigating team decides to carry out the follow-up independently, depending on the importance of the case, its complexity and the expected number of activities needed to investigate the report.

The investigating team may invite specialists, both from inside and outside the organization, including lawyers, psychologists, health and safety specialists and others, to participate in follow-up activities, according to the nature of the case.
If the Report concerns a person appointed to the Investigating Team, that person is excluded from the work concerning that Report.

The Investigating team shall act independently and impartially. It is impermissible to influence the actions of the members of the Investigating team, to give them instructions on how to proceed or to influence the decisions that are issued.

8. What are the follow-up measures?

COMPUTACENTER is obliged to carry out follow-up activities on the Report. Follow-up actions include any actions taken to verify the information contained in the Report and to assess its reliability, completeness and potential consequences and, where appropriate, to prevent the violation of the law indicated in the Report. Such actions include, in particular, the conduct of an internal investigation.

In the course of the investigation, the Investigating team may collect information, request documents, oral or written explanations, analyse IT data and any other information that helps to clarify the case. The work of the Investigating team is covered by corporate confidentiality. All persons with whom the Investigating team interact in the course of the investigation, including those with whom interviews are conducted, are bound by an obligation of confidentiality.

The Investigating team is obliged to provide the Whistleblower with feedback, including, in particular, information on whether or not a violation has been established within **3 months** from the date of confirmation of the Report, or, if it is not possible to confirm the Report, within 3 months from the expiration of 7 days from the date of the submission of the Report.

9. How do we protect whistleblowers?

COMPUTACENTER provides the Whistleblower with protection against disclosure of identity and against any discrimination, retaliation or unfair treatment caused by making a Report (hereinafter: **the Retaliation**).

The Whistleblower shall not be subject to disciplinary, civil or criminal liability as a result of submitting the Report in good faith.

It is forbidden to take any decisions against the Whistleblower that adversely affect their working conditions in connection with the Report, and it is also forbidden to threaten to take such decisions. Such negative decisions include, in particular: refusal of employment, unfavorable change of working conditions or salary, change of position or place of work, withholding of promotion, withdrawal of promotion, withdrawal of bonus or benefit, withholding of trainings or development of career path, termination of employment contract or civil law contract.
Protection shall also apply to a person who assists the Whistleblower. If someone assists the Whistleblower, the Whistleblower should immediately inform the Investigating Entity or the team, indicating what the assistance consists of. The person who assists the Whistleblower is also the person's supervisor, who passes on the information about the violation obtained from the Whistleblower.

It does not constitute the Retaliation to draw consequences against a Whistleblower if he/she is the perpetrator or co-perpetrator of a violation.
If any actions are reported that may constitute the Retaliation against the Whistleblower, COMPUTACENTER will take appropriate steps to eliminate and counteract them (see section 11 below).

10. Who is not subject to protection?

COMPUTACENTER has the right to take appropriate legal action against the whistleblower in a situation where the:

- The Whistleblower had no reasonable grounds to believe that the information about the violation indicated in the Report was true at the time the Report was made;
- The Whistleblower made the Report in order to obtain unauthorized benefits or privileges;
- The Whistleblower's intention was to harm other potential Whistleblowers or to cause harm to **COMPUTACENTER**.

11. What action does COMPUTACENTER take once a violation has been identified?

Measures in the event of a violation may include, in particular:

- application of disciplinary sanctions, in accordance with the Labour Code;
- change of subordination or reporting;
- termination of the contract between COMPUTACENTER and the infringer (in the case of an employment contract, with or without notice);
- initiation of civil, criminal or other proceedings;
- changes in the organisation to minimise the risks of future violations (compliance system, audit, monitoring).

12. Report to public authorities

The Policy does not limit the right to notify the public authorities about a violation of law, including the Ombudsman. A notification to public authorities, including the Ombudsman, may be made orally, electronically or in writing. The detailed policy for the receipt of notifications is set out in the regulations of public authorities and the Ombudsman, available on their websites.

13. How do we process personal data?

The administer of the personal data processed within and in connection with the follow-up activities is **COMPUTACENTER**. Personal data shall be processed in accordance with the General Data Protection Regulation no. 2016/679, the Act of 10 May 2018 on the Personal Data Protection, the Act of 14 June 2024 on the protection of whistleblowers and other data protection legislation, in order to clarify the circumstances described in the Report, to prevent the occurrence of violations, and to draw legal consequences against those guilty of violations.

If personal data is obtained that is not necessary to achieve the above purposes, such data will not be processed and, if obtained, will be promptly deleted as soon as it is determined to be useless.

The Receiving Entity, the Investigating Entity and each member of the Investigating team shall obtain written authorisation from **COMPUTACENTER** to process personal data before performing their tasks.

Data relating to the Report shall be stored in the Report Register maintained by the Investigating Entity. Documents and information collected in the context of the Report and follow-up actions shall be retained by **COMPUTACENTER** for a period of 3 years after the end of the calendar year in which the follow-up activities were completed or after the completion of the proceedings initiated by the follow-up actions.
The policy goes into effect on September 25, 2024 and is available on the website https://www.computacenter.com/en-pl.