4C STRATEGIES

4C Strategies Whistleblower Policy

4C STRATEGIES

Content

INTERNAL AND EXTERNAL POLICY

1. Purpose and Scope

4C Group AB (publ) and its subsidiaries ("**4C**") strives to achieve transparency and always operate at a high level of business ethics. Our whistleblowing channel offers a possibility to alert the organization about suspicions of misconduct in a confidential and, if desired, anonymous way. It is an important tool for identifying potential issues, reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage. Whistleblowing can be done openly or anonymously.

2. Who can raise a concern?

We encourage anyone who becomes aware of misconduct within 4C to speak up. Reporting persons could for example be employees, job applicants, volunteers, interns or trainees, consultants, members of professional bodies, shareholders or persons who have belonged to any of the categories above.

3. When to raise a concern?

The whistleblowing service can be used to alert about serious risks of misconduct affecting people, our organisation, the society or the environment in such a way that it is in the general interest that it becomes revealed. Reported issues could include criminal offences, irregularities and violations or other actions in breach of EU or national laws within a work-related context, for example:

- **Corruption and financial irregularities:** for example, bribes, unfair competition, money laundering, fraud and conflicts of interest.
- **Health and safety violations**: for example, workplace health and safety, product safety, serious discrimination and harassments that are against the law.
- **Privacy violations:** for example, improper use of personal data.

Employees are asked to contact their closest Line manager for issues relating to dissatisfaction in the workplace or related matters, as these issues cannot be investigated in the scope of whistleblowing.

A person who raises a concern does not need to have firm evidence. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service is a serious disciplinary offence.

The protection of reporting persons does not apply if the reporting person reveal classified information.

4. How to raise a concern?

Submit a report through WhistleB

The whistleblowing channel is administrated by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB deletes all meta data, including IP addresses. You will remain anonymous and receive an ID and password that can be used to follow-up on your report and receive messages during the investigation. It is forbidden for

anyone on the Whistleblower Team or investigation team to take any measure to reveal the identity of an anonymous whistleblower. The channel can be reached through this link: https://report.whistleb.com/4cstrategies
By telephone – call +46725738777
Request a meeting – call +46725738777 or send a report through WhistleB to request a meeting.

Remember that the reporting channel is a compliment to regular internal reporting, if you are an employee at 4C and comfortable to do so you can always raise concerns with your line manager.

For reports relating to our Swedish companies, you also have the option to report externally to a competent authority, information about competent authorities for external reporting can be found here.

5. What happens after I raised a concern?

Whistleblower team and investigation team
Access to reports and messages received through our whistleblowing channel is restricted to the appointed Whistleblower Team. Their actions are logged and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process. These individuals can access relevant data and are also bound by confidentiality.

The Whistleblower Team consists of:

Jessica Skytte (Head of Legal & Compliance)
Nina Linder (Group Legal Counsel)

Communication
When you submitted your report, you will receive a confirmation that the Whistleblower Team has received your report as soon as possible but at the latest within seven days.

The Whistleblower Team may not investigate the reported misconduct if:

- ✓ The alleged conduct is not reportable conduct under this *Whistleblower Policy*.
- ✓ The message has not been made in good faith or is malicious.
- ✓ There is insufficient information to allow for further investigation.
- ✓ The issue has already been solved.

If a message includes issues not covered by the scope of this policy, the Whistleblower Team will direct you to the responsible function for the subject matter.

The Whistleblower Team can, when needed, submit follow-up questions via the channel for anonymous communication. The team will inform you of the persons that will receive information about the report, unless that would jeopardise the effectiveness of the measures needed to be taken and subject to considerations of confidentiality such as the privacy of those against whom allegations have been made. The Whistleblower Team will keep you continuously informed, and send appropriate feedback no later than within three months upon the date of receiving the report.

Investigation
The Whistleblower Team will immediately determine if there are any actions that has to be taken to stop on-going misconduct.

- A report will not be investigated by anyone who may be involved with or connected to the wrongdoing.
- Whistleblowing messages are handled confidentially by the parties involved.

The Whistleblower Team will then set up a plan for the investigation of the suspected misconduct. An investigation team with the relevant persons will be appointed (for example if the concern might lead to that a certain employee has to be suspended from his/her employment, HR needs to be involved). The investigation team will be limited to the persons that are necessary to investigate the misconduct or to take the required remedial actions. No person will get more information about the report than required for the part they are involved in. No one from the Whistleblower Team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.

The Whistleblower Team will also determine the potential risk of retaliation and set up a plan of how to prevent retaliation and follow-up with you to ensure no retaliation has occurred.

Once the misconduct you have raised has been remedied the Whistleblower Team will evaluate how the misconduct could occur and what measures we have to take to prevent it from happening again.

6. Protection

4C shall never act in any way to prevent reporting or try to prevent reporting under this policy. A reporting person expressing a genuine suspicion according to this policy should not be subject to any retaliation for example suspension from work, losing their job, discrimination or other disadvantages. Retaliation is also prohibited against any person assisting the reporting person or have a connection to the reporting person such as co-worker or family. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

7. Personal data

4C may, through the whistleblowing service, collect personal data of the person submitting the report (if not sent anonymously), persons mentioned in a report and any third person involved, in order to investigate facts on the declared misdeeds and inappropriate behaviour eligible under the *4C Code of Conduct* or internal rules. This processing is based on statutory obligations and the legitimate interest of the controller to prevent reputational risks and to promote an ethical business activity. The provided description and facts under this processing are only reserved to the competent and authorized persons who handles this information confidentially. You may exercise your rights of access, of rectification and of opposition, as well as of limited processing of your personal data in accordance with the local data protection legislation. These rights are subject to any overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and investigation of the case. For any further questions or complaints please address your request to privacy@4cstrategies.com.

You have the right to report concerns under the GDPR or the UK GDPR to the relevant supervisory authority:

Sweden	Norway	Finland	UK
Integritetsskyddsmyndigheten https://www.imy.se/ +46 8 657 61 00	Datatilsynet https://www.datatilsynet.no +47 22 39 69 00	Office of the Data Protection Ombudsman http://www.tietosuoja.fi/en/ +358 29 56 66700	The information Commissioner https://ico.org.uk/ 0303 123 1113

Controller: 4C is responsible for the personal data processed within the whistleblowing service.

Processor: WhistleB Whistleblowing Centre AB (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm, Sweden) responsible for the whistleblowing application, including processing of encrypted data, such as whistleblowing messages. Neither WhistleB nor any sub-suppliers can decrypt and read messages. As such, neither WhistleB nor its sub-processors have access to readable content.

8. Deletion of data

Personal data included in reports and investigation documentation is deleted when the case is closed and achieved (when the investigation and remedial actions are completed), with the exception of when personal data must be maintained according to applicable laws. Permanent deletion of personal data is carried out 30 days after the case is closed. Investigation documentation and whistleblower messages that are archived will be anonymised under GDPR; they will not include personal data through which persons can be directly or indirectly identified. Documentation is retained for as long as necessary for the appropriate actions and follow up, but will be deleted at the latest two years after the case has been closed.