

## **Policy for Reporting of Infringements Relating to Financial Markets Regulations, Anti-Money Laundering and Terrorist Financing or other suspected irregularities (Whistleblowing)**

### **1.1 Background and applicable laws and regulations**

Verkkokauppa.com strives to act transparently and ethically.

This policy describes how employees, customers and other stakeholders can report activity that they suspect to be contrary to Verkkokauppa.com's ethical guidelines and other corporate policies and that may harm individuals or the company. The reporting methods and reporting channel (Whistleblowing), that give a ways to report suspicions of misconduct or policy violations for internal investigation in Verkkokauppa.com are described below.

Legislation in Finland requires the Company to adopt and implement appropriate internal procedures for their employees to report suspected infringements or violations of applicable laws and regulations relating to financial markets or anti-money laundering. The procedures below are based, among other, the provisions of the Securities Market Act (746/2012, as amended), the EU Market Abuse Regulation (596/2014, "MAR") and the Act on Preventing Money Laundering and Terrorist Financing (444/2017, as amended, "AML Act"). In addition, to the above, Verkkokauppa.com is committed to the highest standards of ethical conduct and full compliance with all applicable national and international laws.

The aim of this policy is further to ensure the proper processing of personal data for the efficient use of the reporting channel.

Verkkokauppa.com Oyj is committed to ensuring that any reported infringements or suspected irregularities are properly dealt with if they do arise. The Company encourages employees to raise their concerns about any misconduct at the earliest possible stage, and this policy sets out the appropriate method for raising any such concerns of infringement.

### **1.2 Reporting methods and reporting channel**

If a person becomes aware of behaviour or practice that is in violation of the company's ethical guidelines and/or other policies or suspects financial malpractice, the person can act as follows:

- **Alternative 1: The employee can report the matter to his/her supervisor (primary)**
  - An employee with a concern about the company should primarily contact his/her supervisor.
- **Alternative 2: The employee can report the matter to the company management or HR-department**
  - If the employee so wishes or the concern relates to the employee's supervisor, a report can be made to the company management or HR-department.
  - In questions of interpretation concerning the employment relation, working environment, HR matters or other similar questions, the employee should contact the HR-department.
- **Alternative 3: The stakeholder can report the matter to contact person at Verkkokauppa.com or company management**
  - The company encourages primarily its stakeholders to discuss the concern with their contact person at Verkkokauppa.com company's representative.
  - If the stakeholder so wishes or the concern relates to the stakeholder's contact person, a report can also be made to the company management.

- **Alternative 4: The employee or stakeholder can report the matter, either with his/her name or anonymously through the reporting channel (Whistleblowing)**
  - The report can be made confidentially by e-mail to the address [compliance@verkkokauppa.com](mailto:compliance@verkkokauppa.com) or by mail Verkkokauppa.com Oyj, Compliance, Tyynenmerenkatu 11, 6 krs. 00220 Helsinki.
  - Primarily, reports should include the name of the person making the report to make further investigation more efficient. If need be, however, anonymous reports may also be submitted.
  - This reporting channel is available to all external stakeholders.

The reported information shall be of sufficient detail to facilitate and enable an investigation of the matter. If the person making a report would like to be informed of the on-going investigation or any measures take as result of the report, contact information should be provided.

### 1.3 Receiving a report

All reports will be treated seriously and handled promptly. Upon receiving a report through the Whistleblowing reporting channel, the whistleblowing team decides whether to accept or decline the report. If the report is accepted, appropriate measures for investigation will be taken.

The whistleblowing team may decline to accept a report, if:

- the alleged misconduct is not reportable conduct under this policy,
- the report is malicious or has not been made in good faith,
- there is insufficient information to allow for further investigation,
- the matter of the report has already been solved.

If a report includes issues not covered by the scope of this policy, the whistleblowing team should take appropriate actions to solve the problem.

Potentially intrusive information of a personal nature, such as health or political, sexual, or religious beliefs will not be included in an investigation. The whistleblowing team has separate protocols to ensure that the persons relating to the report are not included in their handling.

### 1.4 Investigation

All accepted reports of alleged misconduct will be subject to an investigation in accordance with this policy. The whistleblowing team determines the appropriate manner of investigation, allowing for a fair investigation and any necessary corrective action.

- All whistleblowing reports are handled confidentially.
- A report will not be investigated by someone who may be concerned or connected with the misgiving.
- The whistleblowing team will, when needed, submit follow-up questions via the reporting channel.
- No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower by any means.

If the Company decides to launch further investigation on the basis information reported through the Whistleblowing reporting channel, any reported person(s) will be informed of such ongoing investigation and their rights to respond and be heard with respect to allegations, unless informing the person may jeopardize the investigation.

The whistleblowing team consists among other of the Information Security Manager and a nominated deputy. If necessary, the company uses external specialists or resources in the investigations. The

whistleblowing team will periodically report to the Audit Committee of the Board of Director of received reports and on-going investigations.

### **1.5 Whistleblower protection**

Any form of retaliation, including threats or attempts of retaliation against Company's employees who, in good faith and for lawful purposes, report to the Company any conduct or activity that he or she reasonably believes may violate any law or regulation or result in any other wrong-doing, is strictly prohibited.

The Company also prohibits any form of retaliation against employees who provide information, cause information to be provided, or assist in an investigation conducted by the Company or any governmental authority in relation to an alleged violation of any law, rule or regulation applicable to the Company. All officers and managers are responsible for ensuring adherence to this no-retaliation policy.

### **1.6 Treatment of confidential information**

All reports and related information (including personal data pertaining to the reporting and reported persons) will be treated as confidential, except if otherwise provided in applicable law in order to investigate the reported infringement.

Furthermore, any reported information, including but not limited to the identity of the reporting person and the reported person, may be disclosed to the competent authorities, such as the Finnish Financial Supervisory Authority, the Financial Intelligence Unit or the police, in accordance with applicable legislation. Information contained in the reports or otherwise obtained in connection with reporting may be used for internal investigation of the suspected infringements.

The reported information may be accessed and processed within the Company only by such persons, who must as a need-to-know basis have access to the information in order to investigate the report. The Company strives to keep the said group as constricted as possible.

In cases of alleged criminal offences, the whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

### **1.7 Deletion of data**

Any reported information that does not fall within the scope of the abovementioned violations and breaches will be destroyed without undue delay. Any relevant information contained in the reports will be retained for five (5) years, unless further retention is necessary for the purposes of ensuring criminal investigations, pending court proceedings or authorities' investigations or to protect vital interests and rights of the reporting or reported person.

Personal data contained in the reports form a personal data file. The personal data may include e.g. the name and/or contact details of employees or external individuals. A data protection statement (Fi: *tietosuojaseloste*) is available at Company's headquarters at Tyynenmerenkatu 11, 00200 Helsinki or on its website. The data subjects (i.e. the persons whose personal data is in the data file) may have the right to review their personal data contained in the register, unless the review of information would encumber the investigation of suspected infringements. Persons also have the right to have their false or incorrect information corrected or provide a complaint to the Data Ombudsman.

Please also see the Company's guidelines with regard to the general data protection regulation (GDPR).