

Whistleblowing Policy of the University of Turku Approved by the University Board on 20 January 2023

1. General principles

1.1 Background and purpose of the policy

The University of Turku takes all cases of violations, abuse and other inappropriate behaviour seriously. The aim of the ethical guidelines, policies and other instructions of the University of Turku is to ensure that the University's employees act in accordance with the values and instructions of the organisation in all situations, and that they report observed violations or unethical or illegal actions either through the organisational structure or the Whistleblowing Channel of the University of Turku.

This Policy defines the principles and procedures for reporting violations of European Union and national law and the handling of such notifications, as provided for in the act on the protection of persons reporting breaches of European Union and national law (1171/2022, the so-called Whistleblower Protection Act). The Whistleblowing Policy supports the University's responsible operations and compliance with the requirements of the Act.

The University of Turku will not hold the reporting person (henceforth the whistleblower) liable for obtaining or receiving information that has been disclosed or published, provided that such obtaining or receiving is not itself a criminal offence.

1.2 Policy ownership and validity

The Board of the University of Turku has approved this Policy on 20 January 2023. This Policy comes into effect on 1 March 2023.

The Rector decides on further instructions. The Management Support Services unit is responsible for the practical implementation of this matter.

2. Scope of the Whistleblowing Policy

This Policy defines the procedures for handling notifications under the Whistleblower Protection Act. Other internally defined procedures apply to the handling of the whistleblowing cases not covered by the Whistleblower Protection Act.

Reporting a violation and the resulting notification refer to information about a violation or reasonable suspicion of a violation or potential violation of law received by a whistleblower in the course of their employment, duties or responsibilities and the reporting of the violation as described in this Policy. The whistleblower must be associated with the University of Turku by reason of their employment or other contractual relationship.

3. Principles of organising the Whistleblowing Channel and reporting

3.1 Principles of organisation

The Whistleblowing Channel has been designed to protect the identity of the whistleblower in accordance with the legal requirements in all stages of the reporting process. Notifications will be handled by designated notification handlers whose names should be indicated so that a potential whistleblower knows in advance who would handle the notification they submit.

Notification handlers should be familiar with the general principles of disqualification and, if necessary, declare their disqualification to deal with an individual notification.

The University of Turku commits to and ensures that high standards of usability, confidentiality, data protection and security are implemented in the Whistleblowing Channel. The technical implementation of the Whistleblowing Channel will enable confidential communication between the whistleblower and the notification handler in order to solve the notification.

3.2 Reporting

The University Board and the Rector are informed annually of the number and nature of received notifications and of the possible follow-up actions based on the notifications in accordance with confidentiality provisions. In addition, the Board is informed of other notifications that are relevant to the Board's duties or are particularly serious.

4. Protecting whistleblowers

4.1 Conditions for whistleblower protection

A notification submitted to the Whistleblowing Channel ensures the protection of the whistleblower under this Policy. A further condition for the protection is that the whistleblower has reasonable grounds to believe that the information about the violation is accurate at the time of reporting and the reported violation falls within the scope of the Act.

4.2 Prohibition of countermeasures

The University of Turku will not take countermeasures against a person who reports a violation in accordance with the law and the scope and procedures of this Policy. It is also prohibited to prevent or attempt to prevent a whistleblower from reporting information about a violation. Prohibited countermeasures include, but are not limited to, the impairment or termination of an employment contract, layoff, or other adverse treatment of an employee for reporting a violation or suspected violation under this Policy or for participating in the investigation of a reported violation.

Prohibited countermeasures against a partner of the University of Turku include, but are not limited to, the impairment of the terms and conditions of the co-operative relationship, the limitation or termination of the supply of goods or services, or the early termination of the

contractual relationship, or other adverse consequences imposed because the partner has reported violations or suspected violations under the Whistleblower Protection Act or has participated in the investigation of a reported violation.

5 Process for receiving and handling notifications in the Whistleblowing Channel

5.1 Confidential reporting in the Whistleblowing Channel

Reporting through the Whistleblowing Channel is confidential. In the Whistleblowing Channel of the University of Turku, violations are reported in writing, thus ensuring the confidentiality of the handling process and the protection of the whistleblower.

The University of Turku does not undertake to process anonymous submissions, and such submissions are not entitled to the protection of the law.

Persons other than those authorised to process notifications are technically blocked from accessing the Whistleblowing Channel.

A person who has received confidential information may disclose it only if the conditions set out in the Whistleblower Protection Act are met.

5.2 Reporting suspected violations

A notification is submitted through the Whistleblowing Channel available on the University's website.

A notification can be submitted without concrete evidence or full certainty as to whether a violation has occurred. However, a whistleblower who intentionally reports or publishes false information must compensate the subject of the notification for the damage thus caused.

The University of Turku will not hold the whistleblower liable for obtaining or receiving information that has been disclosed or published, provided that such obtaining or receiving is not itself a criminal offence.

If the whistleblower is an employee of the University of Turku, they must assess whether it is proportionate to report the violation in the Whistleblowing Channel, or whether a discussion with their supervisor, a Human Resources representative, a shop steward or someone in the management, for example, is sufficient to resolve the matter. However, the whistleblower always has the option of reporting the violation or suspected violation through the Whistleblowing Channel.

5.3 Recording and storage of notifications

An acknowledgement of receipt of the notification shall be sent to the whistleblower within seven days of the submission of the notification. If the notification is clearly not eligible for processing through the Whistleblowing Channel, the whistleblower will be directed by the notification handlers, in accordance with good administrative practice, to contact the correct place. In this context, the whistleblower should be informed of the implications of the exclusion from the scope of the Whistleblower Protection Act for the notification handling process, the protection of the whistleblower and the confidentiality obligations.

The notification will be deleted five years after its submission at the latest. Other material resulting from the notification (e.g. reports, sanction documents) will be stored or deleted in accordance with the filing plan, information management plan and data protection legislation of the University of Turku.

5.4 Follow-up to the notification

Notification handlers assess the content of the notification and ask the whistleblower for any additional information needed. The task of the notification handlers is to make a proposal for further action and to refer the decision on further action to the Director of Legal Affairs.

If the notification requires further investigation, the Director of Legal Affairs will decide on the appointment of investigators to verify the accuracy of the notification. If the reported violation is found to be fully resolved or further action can otherwise be taken without further investigation, no separate investigators will be appointed.

On the basis of the work done by the notification handlers or investigators, the Rector may decide, on the proposal of the Director of Legal Affairs, to file a criminal complaint, to file another legal claim, to refer the matter to other authorities or to impose internal administrative sanctions of the University of Turku.

The Director of Legal Affairs may decide to close a case when the whistleblower does not provide sufficient additional information through the Whistleblowing Channel upon request. The Director of Legal Affairs may also decide to close a case when repeated notifications are made on the same subject matter without significant new information on the violation when compared to a previous notification already dealt with under the handling process.

The whistleblower will be informed, upon completion of the investigation or at the latest within three months of the submission of the acknowledgement of receipt of the notification, of the actions taken based on the notification.

6. Data protection in the Whistleblowing Channel

The processing of personal data contained in the notifications must comply with the provisions of the General Data Protection Regulation and data protection legislation. Information on the identity of the whistleblower, the subject of the notification and other persons mentioned in the notification and other personal data are principally confidential. This information may be processed by pre-designated notification handlers or designated experts necessary to verify the accuracy of the notification.

Privacy statement and an impact assessment in accordance with legislation and related to data protection and processing will also be maintained of the Whistleblowing Channel. Personal data relating to a notification will be processed for as long as the notification is relevant to the legal content of the notification. The specific retention periods for personal data are defined in the privacy statement.