Whistleblowing

Jari Lahti

Privacy policy, Whistleblowing

Contact

Jari Lahti
Head of Human Resources
jari.lahti@samk.fi
+358 44 710 3130

Grounds for processing

The legal basis is compliance with a legal obligation (Article 6(1)(c) of the GDPR). This obligation is laid down in the European Union Directive on the protection of persons who report breaches of Union law (EU 2019/1937) and in Law 1171/2022 on the protection of persons who report breaches of Union and national law, which transposes the Directive at national level. The notifying person may make the notification under his or her name, but the notification must not contain any other direct identifying information about him or her, such as address details, etc.

If the notifier exceptionally leaves, for example, his/her contact details on the notification form, the processing of personal data is based on the data subject's consent (Article 6(1)(a) of the GDPR).

Purpose of processing

The information sent and received on the Satakunta University of Applied Sciences' notification channel is processed in order to investigate and respond to suspicions of misconduct referred to in the notifications. The investigation of suspected misconduct may require interviews with individuals, documentation of interviews/investigations, decisions on action to be taken in response to the investigation. The processing of personal data is necessary in order to fulfil the obligations of the Directive (EU 2019/1937) identified below to investigate allegations of abuse.

Categories of personal data processed and retention periods

- The categories of personal data processed are:
- first names, surnames, email, public name and username of the processors of the notifications
- notifiers are not required to provide any direct identification information other than their name, but may include their own information about another person/persons as part of the notification, either as part of the written notification or through metadata in the attachments.
- when investigating allegations of wrongdoing, persons who have been involved in the activities to which the allegation relates may be interviewed
- in principle, the personal data to be processed are first and last names and contact details. Other personal data may also need to be processed in connection with the reported suspected abuse.

Storage of personal data:

- notifications are securely deleted from the notification channel service after a retention period of one year, after which the notification is stored in the UAS case management system.
- If there is no statutory retention period for the stored data, the retention periods for the notifications and the data generated by the processing of the notification are determined on the basis of the enforcement and verification of the interests, rights, obligations and legal protection of the natural or legal person; the statute of limitations in tort law and the statute of limitations in criminal law.

Sources of information

- The notifier's personal data, in addition to his/her name, will be obtained from the notifier if he/she provides them.

- the personal data of the third party are obtained from the notifier and, in the case of Satakunta University of Applied Sciences staff, from the controller's files, possibly supplemented by contact details.

Recipients or categories of recipients of personal data

Personal data is received by the authority, if the report requires the suspicion of misconduct to be reported to the authority, possibly by the UAS Board of Trustees, front-line staff, human resources and interested parties.

Data transfer outside the EU/EEA

The data will not be transferred outside the EU or EEA.

Principles of data protection

Access to the data is only available to the processors of the notification channel designated by the controller. Where responses to notifications require preparation, this takes place outside the channel, with access being granted to the persons designated as preparers. Access is limited by user IDs and access rights.

Automatic decision-making

There is no automatic decision-making.

Profiling

Registrants are not profiled.

Rights of the data subject

The data subject has the right under the GDPR to:

- receive information about the processing of personal data, unless an exception is expressly provided for by law
- check the data concerning him or her and correct inaccurate or missing data
- erase their data (not applicable if the processing is based on a legal ground or a task carried out in the public interest)
- restrict the processing of their data
- object to the processing of their data where there is a public or legitimate interest in the processing
- request the transfer of personal data which he or she has provided to the controller, where the ground for processing is consent or a contract
- withdraw his or her consent
- the controller's obligation to notify the rectification/erasure/restriction of processing of personal data
- not to be subject to automated decision-making (the data subject may allow automated decision-making with his or her consent)

The data subject can exercise his or her rights by contacting the contact person or the data protection officer indicated in the notice. For further information on the rights of the data subject, please contact the contact person and/or the Data Protection Officer.

If the processing of personal data does not require the identification of the data subject without further information and the controller is unable to identify the data subject, the rights of access, rectification, erasure, restriction of processing, notification and transfer do not apply.

You have the right to lodge a complaint with the Office of the Data Protection Ombudsman if you believe that your personal data have been processed in breach of applicable data protection legislation. The contact details of the Data Protection Officer can be found on the privacy notices pages. All requests will be dealt with on a case-by-case basis.