

Privacy Notice, Whistleblowing Channel

1. General Information

Kojamo Oyj (hereinafter “Kojamo”) is committed to protecting privacy and processing personal data in accordance with applicable data protection laws and good data protection practices. This privacy notice describes how Kojamo collects, processes, and protects the personal data of (i) the person making the whistleblowing report (“reporter”) and (ii) the person who is the subject of the whistleblowing report. For clarity, Kojamo does not process the reporter’s personal data if the report is made anonymously.

“Personal data” means any information relating to an identified or identifiable person. “Special categories of personal data” means any information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Sensitive data also includes genetic and biometric data for the purpose of uniquely identifying a person, and data concerning health or sexual behavior and orientation. “Processing” means any operation performed on personal data, whether manual or automated, such as collection, storage, organization, and deletion. “Controller” means the entity that determines the purposes and means of processing personal data, either alone or jointly with others.

2. Sources of Data Collection

Kojamo collects personal data provided by the reporter through the whistleblowing channel or other channels. Additionally, during investigations, personal data may be collected from Kojamo’s internal systems and third parties as necessary.

3. Types of Data Collected

Kojamo collects personal data necessary for investigating the case. This may include:

- **Basic information** such as name, email address, and position at Kojamo;
- **Report details**, including all information provided by the reporter, such as the identity of the alleged wrongdoer, description and basis of the alleged misconduct, and any other relevant information;
- **Investigation data**, including all information necessary for investigating the alleged misconduct, such as employment-related information, audit and financial data, information from third-party reports and assessments, and behavior and login data.

Kojamo deletes personal data deemed irrelevant or excessive for the case. Generally, special categories of personal data are not processed in the whistleblowing process. If such data is processed, for example, when necessary for legal claims, the processing is done in accordance with local and EU legislation.

4. Purpose of Data Use

Personal data is used for investigating the reported case and, when the allegation is confirmed, for implementing disciplinary and corrective actions. Processing is based on the following grounds:

- Processing is necessary for Kojamo to fulfill its legal obligations; and
- Processing is necessary to protect Kojamo’s legitimate interests.

Description of Kojamo’s legitimate interest: The whistleblowing channel is a way to monitor the implementation of Kojamo’s ethical principles. The channel allows for the receipt of important and systematic information about potential misconduct and violations and enables timely responses. The existence of the whistleblowing channel supports a good corporate culture by providing employees with a channel to raise concerns and suspicions. Kojamo cannot separately request consent from those subject to the report. Reports can also be made anonymously. Misuse of the whistleblowing system (e.g., maliciously made false reports) leads to consequences, such as disciplinary actions.

5.Data Retention Period

Once the investigation is completed, the case is closed. Material collected during investigations is securely retained until the expiration of the claim period, after which the material is destroyed. In most cases, the material is destroyed within two months (60 days) of the completion of the investigation. The retention period may vary according to mandatory legal requirements, such as laws on occupational safety, corruption, ethics, and accounting. However, data is retained for a maximum of two (2) years after the investigation is completed. If the case proceeds to court and requires a longer retention period, the data is retained for the duration of the legal proceedings. If the allegation is unfounded, the data is destroyed immediately.

6.Access to Personal Data and Disclosure to Third Parties

Personal data is accessed and processed by Kojamo employees who conduct and oversee investigations. Access is limited to individuals who need the data for the aforementioned purposes. The reporter's identity, when known, is not disclosed to the individuals subject to the allegations. The reporter's identity is disclosed only if the reporter consents or if required in criminal proceedings or if the reporter makes a false report with the intent to cause harm. Personal data is disclosed to third parties, such as authorities or external auditors, when necessary.

7.Transfer of Personal Data Outside the EU or EEA

Personal data reported within the EU or EEA is not transferred outside the EU or EEA.

8.Data Subject Rights

Every data subject has the right to request access to their data; request correction or completion of their data if there are errors, inaccuracies, or omissions; request deletion of their personal data; object to processing for reasons related to their particular situation; request restriction of processing; and request their data in a machine-readable format to transfer it to another controller. Note that the exercise of these rights is subject to conditions, and Kojamo may have the right to reject a request. If a request is rejected, the reasons for the rejection will be provided to the data subject. Requests can be sent by email to tietosuoja@kojamo.fi.

9.Contact for Questions Regarding Personal Data Processing

If you have questions about the processing of personal data in the whistleblowing process, contact: tietosuoja@kojamo.fi.

10.Controller

The controller of personal data referred to in this privacy notice is Kojamo Oyj.