PHM Group Notification Channel Privacy Policy

1. General information

In this Privacy Notice, which is based on the EU General Data Protection Regulation (2016/679, "GDPR") and the Data Protection Act (1050/2018), we explain how we process personal data collected through the notification channel (“whistleblowing channel”).
Through the whistleblowing channel, you may, if you wish, anonymously report suspicions or findings of wrongdoing, conduct contrary to PHM Group's ethical principles and violations of the provisions falling in the scope of the Act on the Protection of Persons Reporting Infringements of European Union and National Law (1171/2022), i.e. the so-called Whistleblower Protection Act.
Reports of suspicions can be made by current and former employees of PHM Group, job applicants and stakeholders of PHM Group.

2. Controller

PHM Group Oy (3123812-6) and its group companies ("PHM Group" or "we")

3. Contact details

Postal address: Takomotie 1-3, 00380 Helsinki
Tel. 010 270 8001
E-mail: tietosuoja@phmgroup.com

4. Purposes and legal basis for the processing of personal data

The purpose of processing personal data is to process reports made through the whistleblowing channel and to investigate the reports and take the necessary follow-up action in case of infringements.
The legal basis for the processing is a legal obligation and the legitimate interest of the controller. The provision of a whistleblowing channel and the handling of reports is governed by the Act on the Protection of Persons Reporting Breaches of European Union and National Law (1171/2022). We process personal data primarily on the basis of the controller’s legal obligation.
PHM Group has a legitimate interest in obtaining information about wrongdoing related to PHM Group and its activities in order to investigate it and to ensure the ethical and lawful conduct of PHM Group employees and partners. PHM Group may also utilise information from the whistleblowing channel to prevent misconduct or wrongdoing and to develop its whistleblowing procedures as well as for the purposes of statistical reporting on the use and effectiveness of the whistleblowing channel.

5. Categories of personal data processed

Whistleblowing reports submitted to the whistleblowing channel may contain, and PHM Group may therefore process, personal data relating to the reporting person (if the report is not made anonymously), the subject of the report or any other person (e.g. a witness) who has come to light in the report or internal investigation.
Examples of personal data that may be processed include:

- Name and contact details of the reporting person (if the report is not made anonymously)

- Basic and employment-related information about the subject of the report, such as name, contact details, job title and employer's name
- Other information contained in the report, such as the reporting person's first name, the name and contact details of any witnesses, a description of the misconduct or wrongdoing, the time and place of the reportable event, and any other information the reporting person considers relevant
- Information collected by PHM Group or obtained through internal investigation concerning the notified event or participants
- Information related to the handling of the report, including, but not limited to, the communications that took place in the course of the investigation, the status of the report, and information about the persons handling the report, such as name, contact information, and job title.

The controller may only process data relating to special categories of personal data and to criminal convictions and offences if the processing is necessary for the purpose laid down in Article 1 of the Whistleblower Protection Act. Processing is necessary where the processing is necessary for the establishment, exercise or defence of legal claims. In principle, PHM Group will not process such personal data otherwise. However, PHM Group is not in a position to limit what personal data is processed, as the reporting person can enter the data into the report. The guidelines of the whistleblowing channel ask the reporting person to limit the personal data to only the necessary personal data.

6. Regular sources of the personal data

The primary source of personal data is the reporting person, as PHM Group collects personal data from reports filed in the whistleblowing channel.
PHM Group may also receive personal data from individuals (e.g. witnesses) who may come to light in the course of investigating the reports. Other information necessary for the purpose of processing the report, which may supplement the information contained in the report, includes information obtained from PHM Group's internal systems and registers.

7. Disclosure and recipients of the personal data

PHM Group has acquired the whistleblowing channel as a service from a service provider (NAVEX Global Inc.). PHM Group has contractually ensured that the service provider, as a processor of personal data, processes personal data submitted through the whistleblowing channel in accordance with applicable law.
PHM Group's external experts (e.g. legal services) and public authorities may be involved in the investigation and processing of whistleblowing, to the extent permitted by the Whistleblower Protection Act or other applicable legislation. For example, under the Whistleblower Protection Act, PHM Group may provide information to the pre-trial investigation authorities for the purpose of preventing, detecting, investigating and prosecuting criminal offences.

8. Transfer of personal data outside the EU or EEA

Personal data provided within the EU or EEA will not be transferred outside the EU or EEA, unless otherwise required by mandatory law. If the transfer of personal data outside the EU or EEA is

necessary for the processing of personal data and PHM Group transfers personal data outside the EEA, PHM Group will apply appropriate safeguards, such as standard clauses adopted by the European Commission, to ensure the protection of personal data.

9. Retention period of personal data

PHM Group will delete information received through the whistleblowing channel within five years of receipt of the report, unless retention is necessary for the exercise of rights or obligations under the Whistleblower Protection Act or other law or for the establishment, prevention or defence of a legal claim.

PHM Group will delete without undue delay any personal data that are clearly irrelevant to the processing of the report.

10. Principles of personal data protection

All personal data in the whistleblowing channel will be encrypted, protected and stored in the data centres of an external service provider located in the EU. The whistleblowing platform is certified according to ISO 27001 (Information Security) standards.

Whistleblowing reports and the personal data contained therein are processed only by PHM Group staff members whose job duties require them to do so (e.g. to conduct an investigation or enforce possible sanctions). Persons processing reports are bound by a statutory duty of confidentiality. Access to the whistleblowing channel is restricted to named individuals and protected by user-specific IDs and passwords.

11. Automated decision-making and profiling

PHM Group does not engage in automated decision-making or profiling.

12. Rights of the data subject and their implementation

Unless otherwise provided by applicable law, such as the Whistleblower Protection Act, the data subject has the following rights under the GDPR:

- The right of access to personal data concerning the data subject
- Right to rectification of personal data
- Right to the erasure of personal data
- Right to object to the processing of personal data
- Right to withdraw consent
- Right to restrict the processing of personal data; and
- The right to lodge a complaint with a supervisory authority.

If you are not satisfied with the processing of your personal data by PHM Group, you can contact the supervisory authority, which in Finland is the Office of the Data Protection Ombudsman.

Requests to exercise the rights described above should be made in writing to tietosuoja@phmgroup.com or to the postal address indicated in section 3 of the Privacy Policy.