Reporting channel privacy statement

This privacy policy governs personal data collected through the reporting channel of the Finnish Mutual Insurance Company for Pharmaceutical Injury Indemnities (https://laakevakuutus.ilmoituskanava.fi/#/?lang=en) and processing of such data.

1. Controller

The Finnish Mutual Insurance Company for Pharmaceutical Injury Indemnities (hereinafter referred to as *the Company*), (business ID 2446938-0).

Address: The Finnish Mutual Insurance Company for Pharmaceutical Injury Indemnities, PO Box 115, FI-00181 Helsinki
Telephone: +358 10 219 5712
E-mail: korvaukset@laakevakuutus.com

Communications concerning data protection should be sent to the Company's data protection officer: jenni.valmu@laakevakuutus.com.

2. For what purposes do we process personal data?

The reporting channel receives reports of observed abuses or infringements. These reports include personal data. We only process personal data to discharge the Company's statutory obligations, and when handling reports that we have received.

Processing of personal data is based on the legal duties of the Controller, or on the legitimate interests of the Controller or a third party with respect to the data of third parties, such as data concerning persons subject to a report, and on the consent of a reporting party or in the legitimate interest of the Controller or a third party with respect to data concerning the reporting party. Processing of personal data of persons processing reports is based on a statutory duty or on a legitimate interest.

Reports received by the Company are processed by persons whom the Company has appointed to process reports, and by other persons involved in processing pursuant to the Whistleblower Act (1171/2022) where necessary. The personal data included in a report may only be used for investigating the matter reported.

3. How do we collect personal data?

When submitting a report, reporting parties provide details of the abuse or infringement that they have observed. Personal data on a reporting party are collected in the course of submitting the report, based on the consent of the reporting party and on the legitimate interests of the Controller.

A report may include personal data concerning other individuals if the notifying party considers these details necessary for the purpose of reporting. The reporting form includes a request to avoid submitting sensitive information. Personal data may also be collected in the course of processing a report.

The Controller collects personal data from persons appointed to process reports for the purpose of processing reports and managing access.

Personal data may include such details as a name, address, telephone number, e-mail address, organisation and status, and role in data processing where necessary.

The reporting channel service does not collect identifying information, such as IP addresses or cookies, from a reporting party.

4. How do we process personal data?

Personal data are processed for the purpose of handling reports received through the reporting channel. The Controller takes necessary measures on the basis of reports.

The personal data included in a report are archived in a protected form in the reporting channel service database. The data are only available to the persons whom the Controller has appointed for processing reports. The Controller may limit access to reports according to various report types or the roles of processing staff. The Controller may transfer the data to the Controller's database for the duration of processing or for archiving where necessary. The data are stored in a protected form or in a physically lockable cabinet, to which access is restricted solely to report processing staff.

5. Who may we share personal data with?

Personal data are processed by staff appointed by the Controller to process reports. These staff do not disclose personal data to third parties otherwise than pursuant to a statutory duty, such as when processing of a report results in an official investigation, or if disclosure is necessary to implement measures required by the findings of an investigation of the report.

Personal data may also be shared with third parties in circumstances where impartiality of report processing cannot be guaranteed due to dependencies of staff appointed by the Controller to process reports. To ensure impartial report processing in such cases, the Controller may authorise one or more external processing parties to process the report in accordance with this privacy policy and with statutory requirements. Examples of external processing parties of this kind include auditors, attorneys-at-law, and other independent specialists.

6. Do we transfer personal data outside the European Union? How do we protect personal data?

We do not transfer personal data outside the European Union.

Reports are stored in a protected form.

Only staff appointed by the Controller to process reports receive information from reports and may process them in the service. Each member of the processing staff employs unique user credentials when logging in to process reports. The person responsible for technical maintenance of the system has no right of access to the report database.

Reports and related information are archived in physically locked cabinets. Only appointed report processing staff may access archived data.

7. For how long do we process personal data?

Personal data will be erased and destroyed no later than five (5) years after receiving a report, unless retention is necessary in order to implement statutory rights or duties, or to prepare, submit or defend a legal claim.

The necessity of further retention of data will be examined no later than three (3) years after the previous review. An entry concerning a review is made in the database data.

Personal data that are clearly not relevant to processing a report are erased without undue delay. The report remains in the reporting channel for one (1) year in the form in which the reporting party submitted it. The period of retention in the reporting channel may be prolonged for legal reasons. Reports and their associated personal data are entirely deleted from the reporting channel after the retention period ends. The processing staff erase personal data that are clearly not relevant to a report when transferring it to an archive.

The Controller erases and destroys personal data after processing of the personal data is no longer necessary.

8. Rights of a data subject

A data subject has rights related to the processing of personal data. Rights may be limited in legislation. All restrictions on the rights of data subjects must be based on proportionate and necessary grounds, such as ensuring verification of the accuracy of a report or protecting the identity of a reporting party, and may not restrict the rights of data subjects more than is necessary.

Data subjects are entitled in principle to access their own data unless such access is restricted due to a need to protect essential rights of the Controller or a third party. One example of such circumstances arises when access to data results in a risk of disclosing the identity of a reporting party.

Data subjects have the right to request rectification or erasure of information collected about them. This right of a data subject may also be restricted if the restriction seeks to ensure a statutory duty of the Controller, particularly the duty to provide a reliable and impartial reporting channel.

Data subjects are entitled to request the erasure of personal data collected about them, provided that one of the following criteria is satisfied and that no other legislation or official order imposes a duty to retain the data:

1. the personal data are no longer necessary in relation to the purposes for which they were processed;
2. the data subject objects to the processing in the context of a particular personal situation and there are no legitimate grounds for the processing;
3. the personal data have been unlawfully processed; or
4. the personal data have to be erased for compliance with a legal obligation in Union or Finnish law to which the Controller is subject.

Data subjects are entitled to object to the processing of personal data concerning them. If the Controller processes data on the basis of a legitimate interest, then data subjects are entitled to object to the processing of personal data concerning them on grounds related to their particular personal situation.

If the rights of a data subject have been restricted by law to the extent that is necessary and proportionate to verify the accuracy of a report or to protect the identity of the reporting party, then the data subject is entitled to be informed of the grounds for the restriction, and to request that the information be provided to the Data Protection Ombudsman.

If only part of the data concerning data subjects may serve as grounds for restricting their rights, then the data subjects are entitled to know the other data that concern them.

The Controller generally processes data subject requests within one month. Please contact the address specified in clause 1 of this privacy policy in all matters concerning rights.

A data subject is entitled to submit a complaint to the Data Protection Ombudsman.

9. Do we engage in profiling?

We do not engage in profiling for personal data.

10. Which national legislation governs the processing of data?

The processing of data is governed by Finnish legislation.

11. Right to lodge a complaint with a supervisory authority

Data subjects who consider that their personal data have not been processed in accordance with applicable data protection legislation are entitled to lodge a complaint with the competent supervisory authority or the supervisory authority of the EU Member State where the data subject resides or works.

12. Amendments to the privacy statement

This privacy statement may be updated, for example when legislation is amended. This privacy statement was last updated on 18 August 2023.