Privacy Notice

Our customers' trust is important to us, and we want to process personal data in a way that is worthy of trust. In the processing of personal data, we comply with the General Data Protection Regulation (GDPR), other applicable data protection legislation such as the Data Protection Act 1050/2018 and the Act on Electronic Communications Services (917/2014), as well as with the regulations of the authorities. In our operations, we also ensure the implementation of insurance confidentiality. We ensure the proper and secure processing of personal data with the necessary administrative and technical safeguards.

In this privacy notice we explain how Fennia processes personal data in its operations.

1. Contact information

Fennia Mutual Insurance Company is an insurance company whose field of business includes statutory and voluntary non-life insurances. Fennia acts as a data controller with regard to the personal data it processes in its insurance business and in operations supporting it.

Fennia's contact details:

Fennia Mutual Insurance Company
Kyllikinportti 2
FI-00240 HELSINKI
Postal address: FI-00017 Fennia

The insurance company Henki-Fennia acts as an independent data controller insofar as it processes personal data for the provision of the voluntary life insurance as well as pension and savings insurance services it provides. Fennia acts as a data processor on behalf of Henki-Fennia when Fennia processes personal data for the purposes of insurance provision, risk selection, customer service, insurance and customer relationship management, claims processing, marketing, business development tasks, payment transactions, and risk management.

Henki-Fennia contact details:

Henki-Fennia Insurance Company
Kyllikinportti 2
FI-00240 HELSINKI
Postal address FI-00017 Fennia

In this privacy notice, "Fennia" refers to both data controllers.

The Fennia Group's Data Protection Officer (DPO) can be contacted at tietosuoja@fennia.fi.

2. Data subjects and categories of personal data to be processed

The data subjects are Fennia's:

- insurance and claims customers and potential customers
- insured persons
- beneficiaries
- beneficiaries of the compensation and other parties involved in a claim
- guarantors and pledgors
- persons responsible for organisations and companies
- recourse debtors
- employees, partners, and their responsible persons and employees
- Persons in Fennia's governing bodies such as the supervisory board and boards of directors
- Persons visiting properties owned by Fennia

The processing of job applicants' personal data at Fennia is described in the Recruitment Privacy Notice. Information about the use of cookies can be found here.

The categories of personal data to be processed and their example information include:

Basic information	• Individuals: Name and personal identification number of the data subject. • Organisations: Basic information of persons acting on behalf of the organisation, as well as information about the connection to the organisation.
Contact information	Address, email address, phone number.
Customer due diligence information	Passport number, PEP status information, sanctions check information.
Risk selection information	Credit data, sales ban.
Customer relationship information	Customer identification and categorisation information, including customer ID, insurance ID, customer links such as family, guardianship and representation links, customer segment information and benefit information, and information about memberships that have an impact on benefits or discounts. Pricing-related information such as age, health information, place of residence, claims history, properties of the object of insurance such as a vehicle or apartment, and the extent of insurance coverage selected.
Contract and product information	Data on contracts, products and services between the data controller and the data subject.
Customer transaction data	Tasks and transactions related to the management of the customer relationship, changes in insurance policies, and documentation of tasks related to customers.

Special categories of personal data	• Health information such as health declarations, medical records and medical diagnoses, information about medical examinations and medical procedures carried out. • Trade union membership information.
Billing and collection information	Account number, payment agreement and other billing information.
Financial background information	Data on wages and benefits paid received from official registers, employers or other insurance companies, other financial information.
Data from customer satisfaction and other surveys, interests, customer feedback	Survey responses, interests expressed by the data subject, content of customer feedback.
Consents	Valid consent.
Call recordings and other communication content	Various recordings and messages to which the data subject is a party, such as telephone recordings, online messages, letters, and email and chat conversations.
Claims processing information	Claim report, documents and other information related to the processing of claims, court decisions, information about parties to the claim and compensation information.
Technical identification information	Network identifier information such as cookie identifiers, IP addresses, device and customer identifiers, log data.
Information about convictions and offences	Criminal report, report of an investigation, investigation record, criminal conviction.
Access control information	Video recordings, information collected by electrical door locks.
Data collected by notification channels	Information related to events, errors and anomalies to be reported.
Data from other sources	Data from partners, data collected from open sources.

3. Purposes and legal bases for the processing of personal data

We process personal data for the purpose for which the data was collected, including the management of the customer relationship or to resolve a claim. If we subsequently process personal data for another purpose, we will ensure that the data is not processed for a purpose that is incompatible with the original purpose.

As a rule, we process personal data of children under 12 years of age with the consent of their guardians. Without the consent of the guardians, we only process children's data for certain specific limited purposes. For example, a minor can be registered as a beneficiary of insurance without the consent of a guardian.

Our main purposes for processing personal data and their legal bases are described below.

Establishment and management of insurance customer relationship

The processing of personal data at Fennia is usually based on an insurance contract. We process personal data when we prepare an insurance offer, when the insurance contract enters into force, and when we manage the customer relationship.

Before providing insurance, we determine the need for the policyholder's insurance cover professionally and carefully by processing the necessary information about the object of insurance. Furthermore, before concluding an insurance contract, we check the data subject's credit information. To provide insurance, we also process certain personal data to determine the price of the insurance.

In some situations, we need to process personal data, even if the data subject does not have a contract with us. This is the case, for example, when the data subject is insured or a beneficiary of an insurance policy acquired on their behalf by another person. We also process personal data when a data subject contacts us through a communication channel.

Customer due diligence and sanctions checks

We use due diligence information related to customers and potential customers to prevent, detect and investigate money laundering and terrorist financing in accordance with the Act on the Prevention of Money Laundering and Terrorist Financing, and to bring under official investigation such an act and the offence by which the property or proceeds subject to money laundering or terrorist financing have been obtained. Information obtained solely for the purposes of preventing and detecting money laundering and terrorist financing will not be used for other purposes. We also carry out sanctions checks required by law for each customer, partner and payee before establishing a customer relationship or business relationship and making the payment.

Customer communication and marketing

We communicate and market our services to our customers and potential customers. For example, we communicate about our claims management services, existing customer benefits and partner benefits.

Even if the data subject is not in a customer relationship with us, we may process their personal data to communicate current issues about Fennia and our services such as the kinds of services and solutions we can offer to support insurance or risk management. With the consent of the data subject, we also carry out electronic direct marketing.

Claims processing and claims management services

We process personal data in connection with claims processing, such as when a data subject claims compensation based on an insurance policy they have taken out or is involved in an accident that is processed based on an insurance policy taken out by a company or another person. The data subject may be a beneficiary, injured party, witness or another party in the claims process.

In claims management services, we work with our partners to help our customers manage the claim situation as smoothly as possible. The claims management services currently include the Autoapu 24 h and FenniaHoitaja services.

Recording of calls

We record and store calls with our customer service to verify customer transactions, clarify our responsibilities and develop our services.

Risk selection

We have a risk selection policy in line with our company's mission and business, in which we define the kinds of risks we insure, and on what terms we offer insurances. Risk selection allows us to ensure the profitability of insurance operations.

We process certain personal data to ensure that our customers meet the requirements of our risk selection policy. For example, for corporate customers, we check information related to the person responsible for the company, and before issuing voluntary personal insurance, we may ask the insurance applicant or the insured to complete a health declaration.

We may refuse to enter into an insurance contract in certain circumstances. For example, such a situation may occur if a customer has been entered in the insurance sector's common insurance fraud register due to fraud against insurance companies, or if we have reasonable grounds to suspect that a person is acting on behalf of someone with whom we will not enter into contracts.

Business development and marketing targeting

We process personal data to carry out various business development projects. We analyse personal data to develop better products and services, and to provide our customers with better customer service and experience. We also analyse personal data to develop insurance pricing models and our processes, as well as to target marketing.

Market and customer surveys

We process personal data for the purpose of carrying out and analysing various market and customer surveys. For example, we measure customer experience with various market and customer satisfaction surveys. We also conduct opinion and marketing surveys to develop our business and services in cooperation with our customers. In addition, personal data may be processed for the implementation of prize draws organised in connection with these activities.

Customer segmentation and profiling

Profiling refers to the automated processing of personal data that uses this data to evaluate certain personal characteristics. We analyse personal data to make customer and risk classifications such as customer segmentation. For example, we use analytics in insurance pricing, customer survey targeting, determining the suitability of products for customers, and to provide and market products and services that meet customer needs. External sources such as Statistics Finland's Grid Database are also used in customer segmentation.

Insurance investigation and crime prevention

According to the general principles of good insurance practice and insurance business, combating insurance fraud is part of the insurance industry's social responsibility. Insurance investigation refers to the investigation of insurance events and their circumstances, and suspected cases of fraud. The aim of the insurance investigation is to find out what actually happened in the case. With the aid of the insurance investigation, we aim to reduce the possibility of committing crimes against our business in our own operations by investigating suspicious claims and other matters. If necessary, we will report suspected crimes to the authorities responsible for preliminary investigation.

Common registers of the insurance sector

To combat crime against insurance companies, the insurance industry uses a common claims register and insurance fraud register. The claims register collects information about the claims filed with insurance companies and is intended to prevent the wrongful claiming of compensation from more than one company. Data on persons suspected of having committed or known to have committed a crime against the insurance company is stored in the insurance fraud register. The insurance company may make an entry in the register when the suspected crime has been reported to the preliminary investigation authority or prosecutor.

We disclose information about non-life insurance policies to claims and insurance fraud registers and check the information in these registers in connection with the processing of claims.

The Netso service we use is a check-in portal for insurance sales channels provided by insurance companies and used by agent companies such as car dealerships and inspection stations. The service allows employees of agent companies to conclude an insurance contract for the customer and register the vehicle.

With other insurance companies, we are the controller of the insurance and claims history system (VVH system), through which insurance companies operating in Finland can request and forward the insurance and claims history information necessary to calculate the price of motor liability insurance between the companies. The VVH system's central data repository also allows insurance companies to maintain claims histories for insured vehicles so that other companies can query them directly from the data repository to the extent provided by their mutual agreements.

Maintenance and development of information systems and information security

We process personal data to develop our information systems to better meet the needs of our customers and business, as well as to ensure the secure processing of data. The goal of information security work is to protect the services and data for which we are responsible and to ensure continuity and regulatory compliance in all circumstances.

Establishment, exercise or defence of legal claims

We process personal data to defend our business with various dispute resolution forums such as complaints boards, courts and other authorities.

Implementing the rights of data subjects

We process your personal data when implementing your rights under the GDPR, such as when compiling a copy of the personal data we process about you or deleting your data.

Communication with authorities, reporting, governance and statistics

We process personal data for the purposes of regulatory reporting and internal reporting, as well as for the organisation of Fennia's governance. We also use personal data to generate statistics for various purposes.

Processing of notifications received through notification channels

We use a variety of reporting channels to receive reports of deviations, errors and misuse in our operations. One such channel is the Whistleblowing channel. Data received through notification channels is processed in accordance with our internal processes.

Processing of personal data related to the leasing and security of properties owned by Fennia

We lease properties we own to other companies and organisations. We act as a data controller with regard to personal data related to the management of the lease, and we also arrange access control to the properties. We store the opening data and video recordings of the property's electrical locks.

Processing of personal data of partners' contact persons and responsible persons

We enter into cooperation agreements with our partners and stakeholders to deliver benefits to our customers. We also use partners to provide insurances. We process the personal data of our partners' contact persons, responsible persons and employees to select suitable partners for us and to carry out our partnership activities.

Customer financing for corporate customers

We offer loans and guarantee insurance to our corporate customers. To provide the service, we process the personal data of the customers' responsible persons, guarantors and pledgees.

Business arrangements

We may receive or disclose certain personal data to a third party in a business arrangement. Business arrangements include various business acquisitions and business transfers, as well as mergers and divisions of companies. Personal data may also be processed for the purpose of outsourcing, that is, if we use an external service provider to provide services.

4. Sources of personal data

We receive personal data directly from the data subject, such as based on a customer relationship and by requesting it from elsewhere based on an authorisation or consent. The data subject may give consent for personal data to be requested from health institutions for purposes such as preparing an insurance offer.

We also obtain information from various public registers such as the Tax Administration, Kela, Traficom, Statistics Finland, the Finnish Centre for Pensions, and address information from the registers of Posti Plc and the Digital and Population Data Services Agency. In addition, we obtain information from private service providers such as Suomen Asiakastieto Oy, Vainu and Fonecta. We also use the common registers of the insurance industry as a source of information.

We collect data based on the data subject's activities on our online service website at www.fennia.fi and in the Oma Fennia online service. We use cookies to help us collect this information. You can read more about our use of cookies here.

5. Recipients of personal data

We may disclose personal data to comply with a legal obligation, with the consent of the data subject, or when we have another compelling reason for the disclosure.

To the extent permitted by law, we disclose personal data, for example, between Fennia Group companies to manage the customer relationship, as well as for marketing and risk management, to the authorities to comply with legal obligations, and to the insurance industry's claims and insurance fraud registers. Personal data may also be disclosed to another company if we sell part of our business.

To receive the information we request from public registers or private service providers, we usually need to disclose some of the data subject's identifying information to these parties. For example, to check payment default entries, Suomen Asiakastieto Oy must be given a name and personal identity code.

We only use carefully selected external service providers to assist us in providing services and processing personal data. We only provide these external service providers with data to the extent that is necessary for the services they provide. We always enter into a data protection agreement with the processors we use.

6. Transfers of personal data outside the European Economic Area

In some cases, we may also transfer personal data to organisations in countries outside the European Economic Area (EEA). The EEA area refers to the EU member states, as well as Iceland, Liechtenstein and Norway.

In addition to complying with other requirements of data protection legislation, the transfer of personal data outside the European Economic Area requires us to provide a specific transfer basis, for example:

- an EU Commission decision on the adequate level of data protection in the receiving country
- Standard clauses approved by the EU Commission to be added as an annex to the data protection agreement
- Binding corporate rules for the transfer of personal data to third countries within a corporate group or a group of companies engaged in a joint economic activity.

7. Automated decision making and profiling

The data subject has the right not to be subject to a decision which is based solely on automated processing such as profiling, and which produces legal effects concerning them or significantly similarly affects them. However, if the decision is necessary to enter into a contract with us and is based on legislation or consent, we may make the decision solely through automated processing.

In the case of an insurance application and a claim, we sometimes process the application as permitted by law using an automated decision-making system. We do this so that we can handle this matter as quickly and efficiently as possible. Subjects of automated decision making are notified of it separately in connection with the service that utilises it.

Insurance for some types of insurance is granted using automated decision making if the customer does not have any payment defaults, and their sanctions check is clear. When we

use automated decision making in personal insurance involving the provision of a health declaration, the decision is also based on the information provided by the data subject and our risk selection guidelines.

When we process an electronic claim using automated decision making, we automatically combine the information in our various systems as necessary to process the claim. We also check if any open issues need to be resolved before the compensation issue is resolved. In addition to the information we have, we may also use information obtained from external sources, for example, to compare the information obtained on the scope of the loss with various databases comparing the prices of objects and services. If the amount of loss and the type of event correspond to the normal loss defined by us in the processing system, and no other abnormalities are detected, the system may automatically approve the claim. The data subject may always refer the automated decision to an expert for reassessment.

8. Data retention periods

The storage period of personal data is determined by the purpose of the data. We retain personal data for the duration of the customer relationship, as well as after the end of the customer relationship, to the extent required for the fulfilment of legal obligations, or if we have another appropriate reason for retaining the data.

Examples of our retention periods:

- Information about the validity of motor liability insurance and occupational accident insurance is retained for 100 years. Documents related to an appeal related to insurance will be deleted after 50 years unless they are to be kept for 100 years as information about the validity of the insurance.
- Data on occupational accidents and personal injuries related to motor liability insurance is stored for 100 years.
- Data on environmental insurance is retained for 100 years.
- Recourse debt data is retained for 30 years.
- Portal messages are retained for 3 years.
- Call recordings are retained for 1–5 years.
- Access control data for properties owned by Fennia is retained for 6 months for data collected by electric locks and 21 days for video recordings.

9. Changes to the privacy notice

We will update the privacy notice when there are changes in the processing of personal data. If the change is significant and requires notifications to data subjects, we will notify them of the change directly.

Updated 8 April 2024