Privacy statement

28-4-2026

ævitæ

Met de kracht van aandacht.

Contents

1. Who are we? 3
2. How do we handle your personal data? 4
3. What personal data do we process? 5
4. How do we obtain your data? 10
5. Why do we process your data and what are the legal grounds? 11
6. How do we secure your data? 16
7. How long do we keep your data? 17
8. With whom do we share your data? 18
9. What are your rights? 22
10. Social media 24
11. Profiling and automated decision-making 25
12. Supervision 26
13. Forms and modifications of the privacy statement 27
14. Questions or complaints? 28

1. Who are we?

Aevitae B.V. (hereinafter: Aevitae) is an Authorised Underwriting Agent.

(Aevitae Arbo has its own Privacy Statement.)

Visiting address:	Nieuw Eyckholt 284 (TwinPort) 6419 DJ HEERLEN
Mailing address:	Postbus 2705 6401 DE HEERLEN
Telephone number:	088 - 35 35 763

2. How do we handle your personal data?

Aevitae and its brands handle your personal data with care. In doing so, we comply with applicable (privacy) legislation and codes of conduct, which give further substance to this throughout the sector. Our employees have taken an oath or affirmation, by which they declare that they will act with integrity and reliability. This also includes keeping secret what has been entrusted.

When do we process your personal data?

This privacy statement applies to all personal data that Aevitae's brands process from you if you are a customer, when you visit our websites, use our digital environment or when you contact our customer service. This statement also applies to other situations, for example when you have submitted an application for a product, but have not yet become a customer. Or if your employer has taken out pension insurance or disability insurance with us for you. Or if you are a beneficiary or have been involved as a witness or injured party in a claim. Or when you use our other business services.

3. What personal data do we process?

When you or your employer apply for insurance or other (financial) product or service from one of Aevitae's brands, we ask for your personal data. You or your employer provide this data to us via your/his advisor/intermediary (hereinafter: intermediaries) or directly via, for example, the website, e-mail or telephone.

a. Name and address details

What data we process depends on the contact we have with you:

- When you visit one of our websites or use our digital environment, we collect data about your visit and the use of our digital environment via cookies (see our Cookie Policy: Cookiebeleid | Aevitae).
- If you request information from us, we will ask you to provide your contact details so that we can send the information to you.
- If you become a customer, we will need at least your contact details (name, address, place of residence, telephone number and/or e-mail address). We use this data for the execution of the agreement we have with you.

b. Financial data

If you are a customer of ours, we use your bank account number to make payments and collect the amounts due (premium). In addition, we may have access to your income data if this is necessary for one or more of our financial products.

c. Additional information

For certain products or services, we may need additional information from you, such as your license plate for car insurance or your occupation for income insurance. This information is required to provide our services to you or to assess the risk, set the terms, or evaluate any potential claims. In addition to your personal details and financial information, we may also ask for your gender, date of birth, and, if applicable, your employee number. The employee number may be used for administrative purposes, such as verification within collective agreements with employers or to check insurance rights and coverage.

d. Health data

In order to accept or perform our (additional) insurance and other (financial) services, we need information about your health in certain cases. Sometimes we need information from your doctor. If we need information from your doctor, we will always ask for your permission in advance. Health data is only shared with the medical service.

Collective income insurance
For group income insurance, we process limited health data, such as sick reports, recovery reports, or the extent to which you are incapacitated for work. We receive this information from you, your employer, the occupational health and safety service or the UWV. If we support you and your employer in reintegration, our reintegration staff can also process information about your limitations and possibilities, so that we can responsibly help you to return to the employment process.

Personal injury
In order to be able to assess and handle a personal injury claim, we process your health data. We may share your data with other parties, such as personal injury agencies or the insurer (upon transfer). Our employees only process health data that they need for the performance of the work. Only the medical advisor may process your health data for the purpose of drawing up a medical opinion. The medical advisor can request additional health data from you for this purpose. The medical advisor will only collect health data from other sources after your explicit consent, if necessary with authorization.

Personal and business accident insurance and travel insurance with accident coverage
The medical adviser plays a central role in assessing your health when taking out insurance or claiming benefits due to incapacity for work or an accident. Only the medical advisor and the employees who work under his responsibility may process your health data. If, for the assessment of your application or your incapacity for work, the medical advisor considers it necessary to request health data from others, such as your general practitioner or treating specialist, he/she will Always ask you for permission in advance. The authorization, with which you give this permission, states which health data the medical advisor wants to request and from whom.

By signing the authorization, you give permission. The medical advisor is responsible for storing your health data. When processing health data, we adhere to the Code of Conduct for the Processing of Personal Data by Insurers (Gedragscode Verwerking Persoonsgegevens Verzekeraars) and the medical advisor adheres to the Code of Conduct for Medical Advisors working in Private Insurance Cases and/or Personal Injury Cases (Beroepscode voor Geneeskundig Adviseurs werkzaam in Particuliere Verzekeringszaken en/of Personenschadezaken).

Pension insurance
For group pension insurance, we do not process any health data, except when you claim disability coverage or if you reconsider a previously made choice.

If, for example, you first chose not to participate in the ANW that your employer offers with us, and later still want to participate, we may ask you for health guarantees.

Health insurance
To apply for your basic health insurance, we do not need any health information from you to take out this insurance. We do not use risk selection for acceptance, because the basic insurance is subject to a legal acceptance obligation. The government determines which coverage is included in the basic insurance. If you apply for additional insurance with us, we may request health data from you in order to assess your application. In the case of additional health insurance, we are free to accept or reject your application on the basis of risk selection.

As authorised underwriting agent of a health insurer (EUCARE), we may process data about your health, insofar as this is necessary for the implementation of the basic insurance or the additional health insurance. The processing of your health data will only take place within a special separate unit (functional unit), under the responsibility of our medical advisor. This is a BIG-registered medical specialist. When processing health data, we adhere to the Code of Conduct for the Processing of Personal Data by Health Insurers (Gedragscode Verwerking Persoonsgegevens Verzekeraars).

e. Criminal data

When taking out non-life or individual income insurance, we may ask you whether you, or your coinsured person(s), have come into contact with the police or the judiciary in the past 8 years. If you, or your co-insured(s), have a criminal history, we will assess whether this delay affects your application. We do this to estimate how high the risk is if we accept you as a customer.
You are obliged to answer the question truthfully. We may only use the stated criminal history for the assessment of the insurance application and for an appeal for incomplete compliance with the applicant's obligation to provide information. We may also process criminal data to prevent and combat fraud and abuse.

We process this data on the basis of Article 33 of the UAVG, the Code of Conduct for the Processing of Personal Data by Insurers and the Protocol Incident Warning system for Financial Institutions (PIFI).

f. BSN

In some cases, we also process your Citizen Service Number (BSN). We only process your BSN if we have a legal basis for doing so.

g. Information about your contacts with us

We process data about the contact you had with us in order to be able to see:

- what the contact was about (such as product, advice, offer, service call, message, complaint, information);
- when the contact was, with whom and how (such as by phone, post, chat, our website, email, newsletter, advisor).

We use this data to:

- read or listen to what we have previously been in contact with you about. Then we can speak to you in a more targeted way during the next contact.

When you use the AI agent “Aevi” in your online account, we process the text you enter, your policy and insurance details, and the time of your interaction, insofar as this is necessary to answer your question. The chat history of the AI agent is not stored in your online account and is not visible to you or to our employees; it is accessible only within our Copilot environment for technical management purposes.

Record and save phone calls
We record and store chat and phone calls for:

- improving the quality of our services;
- training and coaching of our employees;
- entering into and performing insurance contracts;
- providing evidence and assessing (the content of) the communication (in the event of interpretation disputes or disagreements about this);
- preventing and combating fraud; and
- complying with legal obligations.

We can also use Artificial Intelligence (AI) to automatically convert recorded telephone conversations into text (speech-to-text) and make a summary of it and also perform analyses to improve the quality of our services.

We do not keep recorded conversations longer than necessary in connection with the purpose for which the conversation was recorded. The retention period differs per purpose for which a conversation was recorded. If a conversation is recorded and still available, you have the right to listen to the telephone conversation or to receive a transcript of it in the event of a dispute about the content of the recorded telephone conversation.

h. Company information

In our business services, we also process personal data such as the names of contact persons, shareholders or UBOs ('ultimate beneficial owner') of a company or entity. Pursuant to the Money Laundering and Financing of Terrorism (Prevention) and Financing Act (Wwft) and/or the Sanctions Act (Sanctiewet) and/or regulations, we must determine who the UBOs of our business customers and our suppliers are. More information about this can be found on the AFM website.

4. How do we obtain your data?

In most cases, we get the data directly from you. In addition to the information we receive from you, we may also receive and process data from third parties, for example from your employer, adviser, another authorised agent, an insurer or reinsurer or other parties such as the Trade Register and the UBO register of the Chamber of Commerce, Statistics Netherlands (CBS), Central Information System Foundation (CIS), National Road Transport Agency (RDW), Credit Registration Office (BKR), the Land Registry (Kadaster), the Insolvency Register, Personal Records Database (BRP), Employee Insurance Implementation Institute (UWV), IDIN, EVR, the government (lists of governments, such as PEP- and sanction lists) and occupational health and safety services (Arbo). But also, for example, from market research agencies, data enrichment agencies and credit reference agencies.

In addition, we may also consult other (public) sources, such as public registers of the Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets (AFM), but also sources such as newspapers, the internet and public profiles of your social media in order to detect or prevent fraud and abuse and to protect Aevitae.

Finally, we process personal data that is publicly available on social media platforms, such as posts, comments, or mentions in which Aevitae or its brands are referenced.

We obtain this data through specialized social media monitoring tools (such as Coosto), which collect and present public posts on our behalf. We also process personal data when you contact us directly via social media, for example through private messages.

Your visit to our websites

We record data about your visit to our websites, for example which pages you have visited, when you have logged in to our digital environment, or which searches you have done. The next time you visit our website, we can better respond to your personal experience. We may also use this data for marketing purposes. We do this, among other things, by placing cookies. We also process your IP address. Since it is possible that our websites place different cookies, we refer you to the applicable cookie statement of the website you are visiting/have visited for information about the specific cookies used.

5. Why do we process your data and what are the legal grounds?

The purposes and legal grounds for the processing of personal data are:

a. The performance of our services

We use your personal data to contact you to find out whether you can become or remain a customer of ours, to discuss the products or services you purchase from us, to make changes to your personal data or to provide you with (financial) insight and action perspective. We may use your data to manage your products (or those of your employer, such as absenteeism insurance), to handle claims and complaints, and, where applicable, to provide information via an AI agent in the secure online environment about the reimbursements applicable under your policy.

We process your personal data for this purpose on the basis of the performance of a contract (Article 6(1)(b) GDPR) and, where applicable, to comply with a legal obligation (Article 6(1)(c) GDPR).

b. Assessing and reducing risks

We also use your personal data to assess and mitigate risks, for example by:

- ensuring good security. Think of usernames, passwords and control questions;
- conducting an internal quality investigation into possible problems and risks and testing whether legislation has been properly implemented;
- knowing our customers (customer research) and thereby ensuring that we remain a healthy company (risk management). We don't just do customer surveys before or at the start of the customer relationship to determine whether we can accept you as a customer. During the customer relationship, we also have to investigate whether you can still remain a customer of ours;
- consulting our incident register (IVR) and the incident registers of the joint financial institutions (EVR), in accordance with the Protocol on Insurers and Crime and the Protocol on the Incident Warning System for Financial Institutions (PIFI) (see below under 3 and 4) if you become a customer of ours, but also if you are already a customer of ours (for example in the case of claim handling);

- creating (statistical and/or scientific) analyses and reports and provide insights at an aggregated level, for example in order to be able to better assess risks. Where possible, we delete the personal data that we do not need when compiling. And we can bundle data at a certain level of abstraction (aggregate), encrypt (pseudonymise) or anonymize.

These processing operations take place on the basis of a legal obligation (Article 6(1)(c) GDPR), for example pursuant to financial supervisory legislation, and/or on the basis of our legitimate interest to prevent fraud and manage risks (Article 6(1)(f) GDPR).

c. Conducting marketing activities

We are happy to keep you informed. For example, with e-mails, newsletters, offers on our website or via social media. Or with personalized advertisements on apps and websites of other parties and social media. We also use your personal data for this purpose.

We can do this by:

- seeing which Aevitae products and services you already use and which you don't. We do this, for example, by using cookies. For more information on this, please see the cookie statements on specific websites of our brands and entities;
- collecting and analyzing your choices and searches when you visit our web pages and open emails, such as the newsletter. For example, you may be interested in participating in the Aevitaal program or interested in health insurance when you visit certain pages of our website;
- combining the data we have collected ourselves with personal data (e.g. an application for another financial product) and general data from other sources (e.g. Chamber of Commerce).

  Would you rather not receive personal offers? Let us know (see further under 9f and 14).

For marketing activities, we process your personal data based on your consent (Article 6 paragraph 1 sub a GDPR) and/or based on our legitimate interest in promoting our services (Article 6 paragraph 1 sub f GDPR). You may object to this at any time.

d. Improving and innovating

We also use your personal data to improve and develop our products and services and thus tailor our offer to your wishes and needs. We do this by combining personal data and analysing it (or having it analysed) and using it for innovations that make use of analyses. In this way, we come up with new ideas in the context of innovations for the benefit of you, your contact with us and your products or our services and thus better solutions. For example, we can:

- resolve the cause of complaints, improve and speed up pages and forms on the website and processes;
- track the data that measures how customers use our services and what the result of a campaign is. And, if necessary, improve things;
- develop new applications, products and services;
- in the context of the management, including testing, of our (new) (administration) systems/applications, ensure that they function properly and thus guarantee the continuity of our services;
- create (statistical and/or scientific) analyses and reports and provide insights at an aggregated level, for example to properly determine the prices of our products and services. Where possible, we delete the personal data that we do not need when compiling. And we can bundle data at a certain level of abstraction (aggregate), encrypt (pseudonymise) or anonymize.

These processing operations take place on the basis of our legitimate interest to improve and innovate our services (Article 6, paragraph 1, subparagraph f GDPR). Where possible, data is aggregated, pseudonymized, or anonymized.

e. Detecting and combating fraud, abuse and improper use

We obtain the personal data that we process in the context of detecting and combating fraud, abuse and improper use from various (public) sources (see section 4). We may also receive information from tipsters or witnesses in this context.

We may also collect information by, for example, conducting technical, tactical and personal investigations. We can call in research agencies to carry out these studies. If there is a personal investigation, we adhere to the rules of the Code of Conduct for Personal Investigation. In the investigation and combating of fraud, abuse and improper use, personal data are also recorded in our Central Events Administration, our own incident register (IVR) and in that of the financial sector (EVR).

Central Event Administration
To safeguard the security and integrity of the various entities and brands within Aevitae, we use a Central Events Administration. This database stores (personal) data that relates to certain events that require our special attention. Data from the Central Event Administration can only be accessed via our Risk Manager(s) or other authorized employees.

EVR
By means of the joint registers of the financial sector (EVR), we can exchange data from entities and brands within Aevitae, with other financial institutions or with external research agencies. In doing so, we adhere to the Insurers and Crime Protocol and the Financial Institutions Incident Warning System Protocol (PIFI). The following are involved in the PIFI:

- the Dutch Association of Insurers (VvV);
- the Dutch Banking Association;
- the Association of Financing Companies in the Netherlands; and
- Health insurers Netherlands (ZN).

IVR
To safeguard the security and integrity of the various entities and brands within Aevitae, we use our own incident register (IVR). This database stores (personal) data relating to certain incidents that require our special attention. Data from this incident register can only be accessed via our Risk Manager(s) or other authorised employees.

If we record your data in these registers (EVR or IVR) in the context of fraud or other forms of insurance crime, we will inform you specifically (which data, why and for how long) in advance. Unless this is not permitted or if it harms the investigation, for example because the police ask us not to inform you in the interest of their investigation.

Do you disagree with this commitment? Then you can object to this or request that your data be corrected or deleted (see further under 9). Please note that you can submit a request to inspect the registrations relating to you in EVR (an overview of registrations) at the Central Information System Foundation (Stichting CIS). The CIS Foundation uses its own privacy and user regulations for this purpose, which can be consulted on the CIS Foundation's website. A request for inspection can be made to us insofar as it concerns a registration made by us in the Central Events Administration, EVR or IVR.

More information can be found in the Code of Conduct for the Processing of Personal Data by Insurers (GVPV) and the Protocol Information Warning System for Financial Institutions (PIFI).

These processing operations are necessary to comply with legal obligations (Article 6(1)(c) GDPR) and to pursue our legitimate interest in preventing fraud and abuse (Article 6(1)(f) GDPR).

f. Business transactions and operations

We may process your personal data if this is necessary in the context of business transactions and the business operations of Aevitae consider, for example, contemplated or actual mergers, acquisitions, transfers of assets in whole or in part (such as mortgage loan claims), financing, contemplated or actual legal proceedings, bankruptcy or restructuring of all or part of the business activities.

The processing of personal data in this context takes place on the basis of our legitimate interest in sound business operations (Article 6(1)(f) GDPR) and, where applicable, to comply with legal obligations (Article 6(1)(c) GDPR).

g. Social media monitoring and customer communication

We process personal data via social media in order to:

- gain insight into public posts and responses about Aevitae and its brands;
- identify and respond in a timely manner to customer questions, complaints, and signals;
- improve our services and communication;
- monitor reputation and customer satisfaction.

For this purpose, we use a social media management tool (Coosto), which processes this data on our behalf. The processing is limited to what is necessary for these purposes.

This processing takes place on the basis of our legitimate interest in safeguarding our reputation and identifying customer inquiries in a timely manner (Article 6, paragraph 1, subparagraph f GDPR).

6. How do we secure your data?

We handle your personal data with care.

We have taken technical and organisational measures to ensure an adequate level of protection and to protect your personal data against loss or unlawful processing. We pay a lot of attention to optimal security of our systems in which personal data is stored. This includes measures to use our websites and IT systems safely and to prevent misuse. But also to the security of physical spaces where personal data is stored.

We monitor the security of our data traffic 24 hours a day. We have an information security policy and provide training for our employees in the field of personal data protection. Only authorised employees, who need access to your data, can view and process your data. Our employees have taken the oath or affirmation, in which they have promised or declared that they will comply with the laws, regulations and codes of conduct and that they will act with integrity.

7. How long do we keep your data?

We do not store your personal data longer than necessary. In some cases, the law determines how long we may or must keep data. In other cases, we have determined how long we need your data on he basis of laws and regulations. We have drawn up a custody policy for this.

Policy/customer files, for example, are kept for at least 7 years after the relationship with Aevitae has ended. For more information about the specific retention periods, please contact us. For health insurance, you can use the Uniform Measure Privacy Statement (UM02) drawn up by Zorgverzekeraars Nederland (ZN).

8. With whom do we share your data?

We only provide personal data to third parties if this is permitted by law and is necessary for the business operations of Aevitae.

a. Inside Aevitae

Are you a customer of one of our entities or brands that fall under Aevitae? Then we can exchange our personal data with one of the other entities/collaborations or brands of Aevitae. Think of EUCARE, our health insurer. We are jointly responsible for a number of processing operations. This may also apply to entities or brands that are not mentioned in this privacy statement, but are covered by Aevitae or EUCARE (such as our healthcare buyer Caresq B.V.). We do this, for example, for administrative reasons, for a responsible acceptance policy or to prevent and combat fraud.

In addition, we exchange personal data between the various departments of Aevitae, for example to process your request or to get an overview of the products and services you have with us. This allows us to provide you with a better service and, for example, you only have to report a change of address once. You may receive offers for other products from the entities and brands covered by Aevitae.

If you do not want to receive offers for other products, you can let us know. Your personal data is also stored in Aevitae's central customer administration. This is done for internal administrative purposes, including matching your data. This means that we check whether the different business units use the same data from you. It is important to check that we have the correct details of you. By measuring data, we can work more efficiently and provide you with a better service.

b. The government

Sometimes we are legally obliged to pass on certain personal data to the government. These include the Tax and Customs Administration, the Employee Insurance Agency (UWV), the Police/Justice, the UBO register of the Chamber of Commerce or regulators such as the Dutch Central Bank (DNB), the Netherlands Authority for the Financial Markets (AFM), the Dutch Data Protection Authority (AP) and the Netherlands Authority for Consumers and Markets (ACM).

c. Advisor/insurance broker

If permitted by law, we may exchange the personal data necessary for the provision of services with your adviser/insurance intermediary. We will do this as long as you have an agreement with us. Sometimes we need your permission for this. Your mediator is responsible for processing your personal data. If your employer has engaged an intermediary or adviser, we will also exchange personal data with them.
For the purpose of activating the digital environment, we may obtain your e-mail address from your advisor/intermediary.

d. Employers

If you are participating in a group scheme through your (former) employer, it may be necessary for us to share certain personal data with that employer. This is done solely for administrative purposes, for example, to verify whether you are (still) employed by the organization in question and whether you are entitled to participate in the group scheme, any contributions, or discounts.

In this context, we may share personal data such as your date of birth, employee number, and policy details with your employer. We limit this exchange to only the strictly necessary information and ensure that it takes place in accordance with the agreements and safeguards applicable to the group scheme.

e. Other insurer(s)

As a Authorised Underwriting Agent of several insurers, we regularly exchange data with insurers. We do this for several reasons arising from our MGA. But also to recover damage or costs that we have reimbursed, for example from your travel insurer if it also offers coverage in addition to your basic or additional insurance, or from the liability insurer of another person who caused the damage or costs.

f. Service providers and companies we work with

We engage other companies to perform services for us that are related to our services. These are, for example, a collection agency, an expertise agency, a notary, a repairer, a reintegration agency, an occupational health and safety service or a reinsurer. We may also share your personal data with your lawyer or agent. We also share your data with the Emergency Center as the provider of (roadside) assistance.

If you have taken out legal expenses insurance, we will share your data with ARAG as the provider of the legal assistance. We make agreements with all parties to guarantee your

privacy. We may outsource the processing of personal data to third parties for maintenance and support functions, for example (IT) service providers. In most cases, these (IT) service providers are considered to be processors, because they do not have independent control over the personal data that Aevitae makes available to the IT supplier in the context of the services. In those situations, Aevitae remains responsible for the careful processing of your personal data.

g. Partijen die betrokken zijn bij zakelijke transacties en de bedrijfsvoering

Parties involved in business transactions and business operations In connection with business transactions and business operations, as explained under 5f we may share personal data with third parties. This may involve parties who are also involved in the business transactions and business operations, such as a counterparty in legal proceedings or financiers in a business transaction. But it can also involve professional advisors of those parties or, for example, a bailiff, if this is necessary for the business transaction or business operations.

h. Central Information System Foundation (CIS)

For a responsible acceptance and risk policy and to detect or prevent fraud, we record your personal data in and consult the Central Information System of the CIS Foundation. In this register, we record your claims, among other things. In doing so, we adhere to the rules of the CIS user protocol and the Insurers and Crime Protocol and the Protocol for Incident Warning System for Financial Institutions (PIFI). We can exchange information with insurers who are affiliated with the CIS Foundation, under strict conditions. We consult this register during the acceptance process and in the event of a claim notification.

More information about this and the privacy regulations of the CIS Foundation can be found on the CIS Foundation website.

i. External Reference Register (EVR)

Financial institutions can record the conduct of (legal) persons that has led or may lead to disadvantage of financial institutions in an Incident Register. An External Reference Register is linked to this Incident register. This External Reference Register contains only reference data (e.g. a name and date of birth or Chamber of Commerce number) to the incident register, which may be included under strict conditions in accordance with the Protocol Incident Warning System for Financial Institutions (PIFI). Every financial institution that is affiliated with one of the participating trade associations has access to (part of) the External Reference Register.

j. Third parties outside the European Economic Area (EEA)

Your data is generally processed within the European Economic Area (EEA). If we share data with parties established in a country outside the EEA or when personal data is processed outside the EEA, we ensure that the protection of your personal data remains adequately guaranteed. For example, we use Standard Contractual Clauses (European model contract clauses). We make clear agreements with parties so that processing takes place in accordance with European legislation. Your personal data is not resold.

9. What are your rights?

a. View or correct data (access and rectification)

You have the right to ask us which of your personal data we process and to have incorrect data corrected. We ask for verification questions or ask for a copy of your proof of identity* in order to identify you. After identification, you will receive a response from us within four weeks. In some cases, we may choose not to provide any information about your health, for example if we think it would be wiser for the GP to provide an explanation. In such a case, we will indicate to you how the information can be shared or requested.

*Identification:
When providing a copy of your ID, you must make your passport photo and Citizen Service Number (BSN) invisible. We also recommend that you indicate on the copy that this copy is intended to exercise your rights in relation to your personal data.

b. Data deletion and the right to 'be forgotten'

In a number of cases and under certain conditions, you have the right to have the personal data that we have about you deleted. This is the case if:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you have withdrawn consent to the processing;
- you object to the processing on good grounds;
- your personal data has been unlawfully processed by us;
- there is a legal obligation to erase the personal data;
- It is personal data of your child, which has been collected in connection with a direct offer of internet services to your child. The right to be forgotten is not an absolute right. We may decide not to comply with your request and not to delete your data, if your request is not based on one of the above grounds; or
- to be able to exercise the right to freedom of expression and information;
- to comply with a legal obligation;
- for the establishment, exercise or defense of legal claims. If we do not comply with your request to have your personal data erased, we will inform you of the reasons why we will not comply with your request.

c. Restriction of processing

If you believe that we are processing your personal data unlawfully, you can request restriction of processing. This means that the data will not be processed by us for a certain period of time.

d. Transfer of the data (data portability)

You have the right to obtain a copy of the personal data that you have provided to us for the performance of an agreement that you have concluded with us or on the basis of your consent. This only concerns personal data that we have received from you and not data that we have received from third parties. The purpose of this right is to enable you to easily transfer this data to another party.

e. Right to object

You have the right to object at any time to the processing of your personal data, which is based on our legitimate interest or the legitimate interest of a third party. In this case, we will no longer process your data, unless there are compelling legitimate grounds for the processing, which outweigh the processing or which are related to the establishment, exercise or defence of legal claims.

f. Unsubscribe from personal offers

You have the right to unsubscribe from newsletters or personal offers via various channels (e.g. email, telephone and post) about our insurance and other (financial) services. In commercial offers, we always mention an unsubscribe option. Our staff may call you for commercial purposes. If you receive a call from us, you can indicate during the telephone call that you no longer wish to be called. You can also contact us yourself and let us know that you no longer want to be called. When we create profiles to make personal offers for products and services that match your personal preferences and interests, you can object to the use of your data for this purpose at any time.

See section 14 for information on how to exercise your rights.

10. Social media

You can choose to chat with us on our website or contact us via our social media pages. This privacy statement applies to the data we receive from you via these platforms. The use of social media is your own responsibility. This privacy statement does not apply to the way in which social media platforms handle the personal data you provide. Please note that many social media platforms are located outside the European Union and store data outside the European Union. The privacy legislation of the European Union usually does not apply. We recommend that you consult the privacy statement of these social media channels for more information about how they process your personal data.

11. Profiling and automated decision-making

Profiling

We can create profiles of our customers based on the data we collect, with the aim of analysing this data and in this way, among other things, managing risks, making connections and gaining insight into (future) actions and preferences. We can then respond to that. We can do this to improve our services and the range of products and services and to tailor them to your wishes and needs. For example, by using this data to estimate the premium or to send customers targeted advertising/information.

We can also use Artificial Intelligence (AI). We comply with legislation and regulations. This means, among other things, that we ask for permission in advance if this is required by law. For example, in the case of profiling on the basis of special personal data.

Automated decision-making

To assess an application for insurance or a claim report, we sometimes use an automated process. We do this to help you faster and better. When you submit an application, the information you have entered is automatically checked against our acceptance criteria. This allows us to make a risk assessment of your application.

In the event of a claim report, the information you have entered may be automatically checked against our damage assessment criteria, in whole or in part. This allows us to check whether damage is covered. In both processes, we check whether the data is correct and the decision is made on the basis of, among other things, the data you enter, risk data, fraud data and data from (public) sources such as the CIS database.

If the outcome is that the application can be accepted or that the damage can be paid out, then the application will be automatically accepted or the claim will be paid out automatically. You have the right to submit an automatic decision to an employee and receive an explanation. You have the opportunity to let us know what you think and to object to an automatic decision.

In principle, your data will be processed automatically if you apply for basic or supplementary health insurance. This is done on the basis of the information you have entered on the (electronic) application form. In addition, authorisation applications and declarations go through a careful process, in which it is assessed whether your application or declaration falls under the insurance conditions.

The testing of these criteria can be automated. You will always receive a message in which the application or declaration is approved or rejected. You have the right to submit an automatic decision to an employee and receive an explanation. You have the opportunity to let us know what you think about it and to object to an automatic decision.

12. Supervision

A number of authorities supervise how we process personal data:

- The Dutch Data Protection Authority (AP);
  monitors compliance with the GDPR.

- The Netherlands Authority for Consumers and Markets (ACM);
  supervises compliance with the Telecommunications Act (including cookies and direct marketing).

- The Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets (AFM);
  generally supervise the financial sector.

- The Data Protection Officer
  The Data Protection Officer of Aevitae can be contacted by the entities mentioned in this privacy statement (see further under 14).

13. Forms and modifications of the privacy statement

As a member of Zorgverzekeraars Nederland (ZN), we also adhere to the Uniforme Maatregel Privacy Statement (UM02) drawn up by them, but we have taken our own variant, because we do not only offer health insurance. In addition, privacy legislation is always changing. We may therefore amend this privacy statement to remain up-to-date. We do this in the event of new developments, for example if something changes in our business activities, in the law or in the judiciary. We therefore recommend that you regularly review this privacy statement when visiting one of our websites. The latest version can always be found here. The date of the last change can be found at the top of this statement.

14. Questions or complaints?

Questions

Do you have any questions, for example about this privacy statement, or would you like to exercise your rights? If so, you can always contact us through any of these available channels:

Data Protection Officer for Aevitae B.V.

- Van Gelder FG diensten
  Name: Mevr. mr. Marieke van Gelder
  E-mail: privacyrecht@vangelderlegal.nl
  Phone: 088 - 88 40 801

Complaints

Do you have complaints about privacy? Then you can contact:

- Compliance Department
  E-mail: compliance@aevitae.com
  Address: P.O. Box 2705, 6401 DE HEERLEN

- Dutch Data Protection Authority
  Web: www.autoriteitpersoonsgegevens.nl
  Phone: 088 – 18 05 250

For other complaints, please contact:

- Complaint management
  E-mail: klachtenmanagement@aevitae.com
  Address: P.O. Box 2705, 6401 DE HEERLEN

For the privacy statements of our principals, please refer to their respective website and privacy statement.

We would also like to refer you to our website: www.aevitae.com.