

Privacy statement

Version April 2023

This Privacy Statement was last updated on April 1, 2023. This is a translation of the original Dutch text. In the event of any disparity between the Dutch original and this translation, the Dutch text will prevail.

ABN AMRO Verzekeringen and your personal data

This Privacy Statement sets out how we handle your personal data. You can be confident that we handle your personal data with due care.

Who is this Privacy Statement intended for?

Are you a client of ours or have you shown an interest in a specific product, for example by making an application? If so, we use your personal data and this Privacy Statement applies to you. It can also happen that we process personal data relating to individuals who do not have a contract with us, for instance, if you have been involved in a claim made by one of our clients

Who is responsible for your data?

ABN AMRO Verzekeringen (AAV) is responsible for your data. ABN AMRO Verzekeringen is a joint venture between NN Group NV and ABN AMRO Bank NV and is part of NN Group NV. ABN AMRO Verzekeringen is the trading name for ABN AMRO Schadeverzekering NV, ABN AMRO Assuradeuren BV and ABN AMRO Verzekeringen BV. This Privacy Statement applies to these four companies. ABN AMRO Levensverzekering N.V. merged with Nationale-Nederlanden Levensverzekering Maatschappij N.V. with effect from April 1, 2023. For information on how Nationale-Nederlanden Levensverzekering Maatschappij N.V. handles your personal data, please refer to the Privacy Statement of NN Group (Privacy Statement NN).

For retail insurance ABN AMRO Bank usually acts as a broker. For commercial insurance ABN AMRO Verzekeringen itself (usually) acts as the broker. It may also be the case that you take out retail insurance with us through another broker.

What is personal data?

Personal data is information that says something about you. The best known types of personal data are your name, address, email address, age and date of birth. Personal data also includes your bank account number, your phone number and IP address. There are several special categories of personal data. For instance data concerning your health.

The collection, storage and use of your data are referred to as personal data 'processing'. That is a legal term. We process your personal data strictly in accordance with all laws and regulations, including the provisions of the General Data Protection Regulation (GDPR) and the Personal Data Processing Code of Conduct for Insurers.

Personal data we obtain from others

We also use personal data that we have obtained from sources other than yourself. If, for instance, your partner includes you in an insurance application, we can ask for personal data about you. Data may also be obtained from other sources. Think, for instance, of:

- ▶ public registers containing your data, such as the Land Registry and Chamber of Commerce registers;
- ▶ public sources such as newspapers, the internet and public sections of social media accounts;
- ▶ databases of other parties who have collected personal data about you, such as market research agencies or trade information agencies. In this context, we also mention Stichting CIS, which manages an external registration system for insurers, and Credit Reference Agencies;

- ▶ intermediaries and advisers whose services you have enlisted and with whose help you have taken out an insurance policy with us;
- ▶ insofar as your employer has arranged your loss of income insurance through us, we also receive personal data about you from your employer.

On what basis do we process your personal data?

Obviously, we may not request or use your personal data without good reason. By law, we are permitted to do this only if 'the processing has a basis'. This means that we may only use your personal data for one or more of the following reasons:

Contract

We use your personal data for the conclusion and performance of insurance and other contracts with you. We use all sorts of personal data from you in order to perform the insurance contract. These include your address, email address, bank account number and date of birth. In some cases it may also include your car registration number or the composition of your family.

For some types of insurance (e.g. accident insurance products) we also process your medical data. We obtain these personal data from you or - with your authorization - from a doctor. The processing of your medical data takes place under the responsibility of our medical adviser (doctor). Medical data are only provided by the medical adviser to other employees within our company if this is necessary for the performance of their duties. In such cases these other employees are subject to the same confidentiality obligation as the medical adviser on the grounds of doctor-patient confidentiality. To make risk assessments for non-life insurance products, we may also request and process information about any criminal history you might have.

Legal obligation

Insurers are required to adhere to many laws and regulations. European and Dutch rules, but sometimes also rules from other countries. Based on these rules, we process data about you, for instance to establish an accurate picture of you as our client. We also take measures against fraud, tax evasion, terrorist financing and money laundering. This obligation also requires us to verify your identity so that we can prove that we know who you are. For this reason, we may keep a copy of your valid identity document.

Legitimate interest of ourselves or others

We also have the right to use your personal data if this is in our interest. This is referred to as a 'legitimate interest'. For this to apply, our interest in using your personal data must effectively outweigh your right to privacy. In situations such as these, we consider every possible interest.

When do we have a legitimate interest in using your personal data? Examples:

- ▶ To protect our own financial position and that of others. Think, for instance, of measures to prevent and fight fraud. Not just fraud against us, but also against other financial institutions. We can exchange data with these other financial institutions for this purpose. We can also record these data in a separate database within our group or in an external register. Any personal investigation that we conduct in connection with a claim or insurance application is performed in accordance with the Personal Investigation Code of Conduct.
- ▶ Insofar as necessary for the performance of a contract, we can record data of persons other than our clients, such as injured parties, administrators and beneficiaries.
- ▶ To keep improving our risk assessments, product development and product pricing. This means that we use your data for statistical purposes.
- ▶ We keep your data in order to have access to the correct information in the event of a complaint or dispute.
- ▶ To improve our services. For instance, by making efficiency improvements to our accounting systems through centralization, improving customer experience, outsourcing to external service providers or performing statistical and scientific research. We may use Artificial Intelligence for this purpose.
- ▶ For marketing, communication and innovation activities. In these cases, we use information for analyses, including data analyses, and for innovations that utilize data analysis, such as the development and testing of applications in the area of artificial intelligence (AI). We do this to improve our processes and the product and service offering and better tailor it to the needs and wishes of existing and potential customers. Or to improve how our website works and to offer advertisements

that may interest you. For further information, please see our Cookies Statement on our website.

- ▶ Someone else may also have a legitimate interest for which we must use your personal data. If you have had a car accident, for instance, we will need to pass on your data - such as your car registration number - to the other party's insurer in order to settle the claim.

Other purposes

We may use your personal data for other purposes than the purpose for which you supplied the personal data to us. In that case, the new purpose must be in line with the purpose for which you initially provided your personal data to us. The law refers to this principle as 'compatible use of personal data'. The law does not specify exactly when a use is compatible, although it does provide guidance.

- ▶ Is there a clear correlation with the purpose for which you initially provided the personal data? Is the new purpose appropriate to the initial purpose?
- ▶ How did we originally receive the personal data? Did we obtain the personal data directly from you or in another way?
- ▶ What types of personal data are being collected? Is the personal data in question considered sensitive to a greater or lesser degree?
- ▶ What are the consequences for you? Will you benefit, suffer or neither?
- ▶ What can we do to ensure the highest possible level of protection for your personal data? Examples include anonymization and encryption.

Required personal data

If we need personal data from you in order to conclude a contract with you, and you refuse to provide these data even though this is required by law, we cannot enter into a contract with you, or, if a contract already exists, we must terminate our contract with you. The required personal data is specified in the online forms and other forms we occasionally need you to complete.

Do you want us to remove your personal data from our systems? Unfortunately, we cannot remove required personal data. We need this data. For instance, in order to perform the contract you have with us or because we are obliged to retain this data by law or because of a legitimate interest of the insurer.

Camera images, telephone conversations and chats/video chats

Your voice may be recorded during a telephone conversation. Video chats or camera images may also be recorded. We handle such images and voice recordings with due care. They are subject to the same rules as other personal data. You also have the same rights. We can decide to record and retain these telephone conversations, chats/video chats or images. Either to meet legal obligations or to provide evidence or for staff training and appraisal purposes.

Other parties using your personal data

There are situations in which we need to provide your personal data to other people and entities involved in the provision of our services. These are described below.

Our service providers

We occasionally work with organizations that help us provide services to you. This is referred to as outsourcing. Special legal rules apply to outsourcing by insurers. These organizations may also need your personal data to effectively perform the duties they do for us. We handpick these organizations. We make clear arrangements in a contract about how they handle your personal data. Even if we outsource certain services, we will still continue to bear responsibility for them. We may also use third-party services for the settlement of claims. For instance, we can engage an expert to perform an on-site investigation of a fire claim or a medical adviser to investigate the physical consequences of an accident. Within NN Group NV (of which we form a part), we are allowed to share your data for internal administrative purposes or to improve our services to you. We may also share your data in the interest of combatting insurance fraud.

Intermediaries

You may have taken out one of our retail insurance products through an intermediary. This is usually, but not necessarily, ABN AMRO Bank. Intermediaries process your personal data and are responsible for the use of these personal data. For more information about the use of your personal data by an intermediary, you can always consult the website of this intermediary to find out more about how they handle your personal data.

Authorised public bodies

Government bodies such as the Tax and Customs Administration Services, the Public Prosecution Service, public investigation bodies and our own supervisors can request us to provide data. We are obliged by law to comply with these requests, which may include personal data of yours.

External parties

We can share your personal data with external registers such as CIS and the Dutch External Reference Register (EVR). We can also share your personal data with bailiffs, debt-collection agencies and/or civil-law notaries and credit reference agencies (such as EDR). Or with other insurance companies, including reinsurers and legal expenses insurers. We do this insofar as necessary for performing the contract or where there is a legitimate interest in doing so.

Third parties with a legitimate interest

We can also provide your personal data to third parties if they have a legitimate interest in accessing this information. If you have a car insurance claim that must be arranged with the other party's insurer, your personal details will clearly also be supplied to that party. This is unavoidable.

Use of your personal data for direct marketing purposes

If you have previously purchased a product or service from us, we would like to offer you our own similar products and services that suit you as well as possible. You receive offers and news items that suit you and therefore as little advertising as possible about products that you probably do not want or already have. We use personal data that we have received from you. For example because you have ever requested information or because you are already a customer with us. We may also use personal information that we have received from others.

Profiling

As an insurer, we make use of profiling. Below you can read what we do this for and when.

Fraud prevention

We have a great deal of knowledge and experience in the area of fraud prevention. Unfortunately, we are faced with increasingly sophisticated forms of fraud. To find out behaviors or signals that are typical of specific types of fraud, we observe the exact sequence of events leading up to insurance fraud. This allows us to create a profile that we use for identifying and investigating certain activities in more detail. We may use artificial intelligence (AI) for this purpose. We can then take measures to counter fraud as effectively as possible. We can also pass on your personal data about, for instance, a claim or fraud to external warning registers which can also be accessed by other financial service providers. Based on the Protocol Incident Warning System for Financial Institutions (PIFI), ABN AMRO Verzekeringen registers data in the Incident Register of natural persons or legal entities that have led or could lead to affecting AAV, our customers or employees or those that could harm the integrity of AAV. The registered data in the Incident Register can be exchanged with other financial institutions, for example, within the framework of rules dictated by PIFI, for research into fraud, amongst other things. Through the External Referral Register, attached to our own Incident Register, other financial institutions can receive a signal prompting them to look into an application or claim. Further information on this warning system and how it works can be found at www.stichtingcis.nl.

Client acceptance

Profiling can take place when you wish to take out an insurance product with us. We as an insurer can, for instance, apply profiling to make a risk analysis in the case of paper/online insurance applications. In our experience, certain aspects can indicate whether a client or prospect is likely to submit a higher-than-usual number of claims. The insurer looks at these characteristics when you apply for an insurance. A profile is drawn up based on these characteristics.

Automated decision-making

In some cases, we assess your application or claim via an automated process. We may use AI for this purpose. Based on the information you have given, we automatically test whether you meet our acceptance or claim criteria. Amongst other things, we look at whether the data you have given about yourself or the items being insured is correct. We also check your application against fraud indicators and make a risk assessment based on your data and data from other public sources. This check can have consequences for the amount of your insurance premium. You can object to an automated decision and request a reassessment by one of our employees. If you are listed on a fraud register, one of our employees will always assess your application.

Personal data protection

We go to great lengths to protect your personal data as best we can. We invest heavily in our systems, procedures and people. We make sure that our working methods are appropriate to the sensitivity of your personal data. We train our employees to handle your data safely and in accordance with their confidentiality obligation. Only employees who need to view your personal data for the performance of their duties have access to your personal data. We continuously monitor the security of our data traffic. Action is immediately taken when anything goes wrong. Data breaches are resolved and recorded. We are obliged to do this by law. We report this to the supervisor as well as to you if necessary.

Your data outside Europe

Your personal data are usually processed within the European Union (EU). In some cases personal data are processed outside the EU. Some of our suppliers and partners are also based outside the EU or extend these services outside the EU. The regulations in these countries do not always offer the same protection of personal data as European regulations. To ensure that your personal data remain safe in such cases, we conclude agreements providing for the same level of personal data protection as applicable within the EU.

How long do we keep your personal data?

In principle, we keep personal data for as long as necessary for the purpose for which we obtained the personal data. The period for which we keep the personal data, which is referred to as the retention period, depends on the following criteria:

- ▶ The General Data Protection Regulation does not specify concrete retention periods for personal data. Other legislation may specify minimum retention periods, however. If so, we are under the obligation to observe these periods. Think, for instance, of tax legislation or specific legislation for financial companies (Financial Supervision Act). In most cases, we retain your personal data for up to 7 years after your insurance with us stopped or for up to 7 years after your claim was settled.
- ▶ We may become involved in a court case or other legal proceedings, either in the Netherlands or abroad. We retain data so that we have strong evidence to prove exactly what happened. We may keep personal data in our archives until a claim is barred by the lapse of time and legal proceedings can no longer be lodged against us.

What rights do you have?

Right of inspection, right to rectification, right to be forgotten, right to restriction

You have a right to request an overview of all your personal data that we process. This entails that you can ask what personal data we have recorded and the purposes for which these personal data are used. You can request us to rectify any personal data that are not correct. In some cases, you can also ask us to delete your personal data. This is not possible in all cases. Nor are we always obliged to grant a request to delete your data. Sometimes, for instance, the law obliges us to retain your personal data for a longer period.

You can also ask us to restrict the use of your personal data on a temporary basis. This is possible in the following situations:

- ▶ You think your personal data is incorrect;
- ▶ We are not supposed to use your personal data;
- ▶ We want to destroy your personal data, but you need it (for instance after the retention period).

Right to object

You can object to the processing of your personal data if, in your opinion, we use your personal data for purposes other than those necessary to perform a contract or to comply with a legal obligation. We make a careful assessment of your objection and stop the processing of your personal data if necessary.

Right to data portability

We can make sure that you receive the personal data you have provided to us and that we have entered into our automated systems for the purposes of performing an agreement. This is referred to as data portability. You can also request us to send these data directly to another party.

Please keep your personal data safe and secure. We urge you to check whether any party you want to provide your personal data to can be trusted and keeps your personal data as safe as we do. If you want to receive your personal data, make sure that your own equipment is safe enough and is not prone to hacking. Your financial information may be worth gold to criminals. A request to receive or send your personal data to another party can be submitted via klantrechten@nl.abnamro.com.

Exercise your rights

If you wish to exercise one of the above rights, you can send a request to dpo@abnamroverzekerings.nl. You must provide your request with your name, address, telephone number, policy number and a copy of a valid proof of identity, where the BSN number and passport photo should be shielded. We appreciate it if you inform us of the background of your request, so that we can help you as specifically as possible.

Do you have a complaint or want to ask a question?

We have a designated Data Protection Officer. You can reach him or her via dpo@abnamroverzekerings.nl. If you have any questions about the Privacy Statement, you can contact our Data Protection Officer. If you disagree with how we handle your data, you can also submit a complaint via dpo@abnamroverzekerings.nl. Alternatively, you can submit a complaint to the Dutch Data Protection Authority (www.autoriteitpersoonsgegevens.nl).

Changes to the Privacy Statement

Changes in the use of personal data may occur over time as a result of changing laws and regulations or changes to our services and products that have direct consequences for our use of your personal data. In this case we will amend the Privacy Statement.