a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Privacy Statement ASR Nederland N.V.

10-2023

Click on the titles below to go to the relevant subject

Table of contents

1 Who are we? >>
2 How do we handle your personal data? >>
3 Which personal data do we process? >>
4 How do we obtain your data? >>
5 Why do we process your data? >>
6 What is the legal basis for using your personal data? >>
7 How do we secure your data? >>
8 How long do we retain your data? >>
9 With whom do we share your data? >>
10 What are your rights? >>
11 E-mail and social media (chat, WhatsApp, Facebook) >>
12 Profiling and automated decision-making >>
13 Supervision >>
14 Amendment of the privacy statement >>
15 Any questions or complaints? >>

back to contents >

Privacy Statement ASR Nederland N.V.

1. Who are we?

ASR Nederland N.V. is the point of contact for the processing of personal data by the following entities and brands (a.s.r.): ASR Levensverzekering N.V., ASR Basis Ziektekostenverzekeringen N.V., ASR Aanvullende Ziektekostenverzekeringen N.V., ASR Schadeverzekering N.V., ASR Vermogensbeheer N.V., ASR Real Estate B.V., ASR Vitaliteit en Preventieve Diensten B.V., ASR Vooruit B.V., ASR Premiepensioeninstelling N.V., ASR Re-integratie B.V., Aegon Hypotheken B.V., Aegon Levensverzekering N.V., Aegon Cappital B.V., Aegon Advies B.V., Aegon Bemiddeling B.V., Aegon Administratie B.V., Aegon Administratieve Dienstverlening B.V., Aegon Spaarkas N.V., a.s.r., Aegon and Loyalis.[1] [2]

Visiting address:
Archimedeslaan 10
3584 BA Utrecht

Postal address:
PO Box 2072
3500 HB Utrecht

Facebook
Twitter

(a.s.r.) WhatsApp: +31 (0) 623889539
Telephone: +31 (0) 30 257 9111

a.s.r. Vitality and a.s.r. Real Estate have their own privacy statement.
For more information, see: www.asr.nl/vitality/privacy and asrrealestate.nl/privacy-statement

2. How do we handle your personal data?

ASR Nederland N.V. and its brands handle your personal data with due care. In doing so, we comply with applicable (privacy) legislation and codes of conduct that further specify this across the sector. All our employees have taken an oath or have made a solemn affirmation to act with integrity and reliably. This also includes: keeping confidential what has been entrusted to them.

When do we process your personal data?
This privacy statement applies to all your personal data that the brands of ASR Nederland N.V. process when you are a customer, when you visit our websites, when you use our apps or the 'My platform', or when you contact our customer service desk. This statement also applies to other situations, for example if you have applied for a product but have not become a customer. Or if your employer has taken out pension insurance or disability insurance for you with us. Or if you are a beneficiary or have been involved in a claim as a witness or an injured party. Or if your partner takes out a mortgage with a.s.r. and you will also be living in the house. Or when you make use of our business services.

1 And the brands that are no longer used, insofar as personal data are still being processed, such as: Ardanta, Ditzo, Europeesche Verzekeringen, ZZP Pensioen, De Amersfoortse, Axent, De Eendragt, Generali Nederland.

2 Aegon Nederland N.V. merged with ASR Nederland N.V. in October 2023 and this privacy statement applies to the aforementioned Aegon entities. Aegon Schadeverzekering N.V. merged with ASR Schadeverzekering N.V. in October 2023.

back to contents >

3. Which personal data do we process?

When you or your employer applies for insurance or other (financial) products or services from one of the brands of ASR Nederland N.V., we will ask for your personal data. These data will be provided to us by you or by your employer via your or its adviser/intermediary (hereinafter: financial service provider) or directly, for example via the website, email or by telephone.

a. Name and address details

Which of your data we process, depends on the contact that we have with you:

- If you visit one of our websites or use our app, we collect data about your visit and app usage by means of cookies.
- When you request information from us, we ask you to provide us with your contact details, which allows us to send you the information.
- When you become a customer, we will in any case need your contact details (name, address, telephone number and/or email address). We use these data to implement the agreement that we have concluded with you.

b. Financial data

If you are a customer with us, we will use your bank account number to make payments and collect the amounts due (contribution, fee, periodic deposit or interest). In addition, we may have access to your income details if this is necessary for one or more of our financial products.

c. Additional data

For some products or services we will need additional information from you, for example your car registration in case of a car insurance or your profession in case of an income protection insurance policy or mortgage. We need these data in order to provide services to you or to assess the risk, determine the conditions or evaluate possible claims. In addition to the name and address details and the financial data, we may also ask for your gender and date of birth if this is necessary for our services.

d. Health data

In order to accept or implement our insurance policies (which also include the handling of personal injury claims) and other (financial) services, in certain cases we will need information about your health. Occasionally we may need information from your physician. If we need information from your physician, we will always ask for your prior consent. With regard to health data, these are only shared with the medical service.

Funeral insurance/Life insurance

We ask health questions when we receive applications for our funeral insurance and in certain cases for life insurance . These are shared with an a.s.r. medical adviser via a secure environment, so that we can assess whether we can insure the risk.

Group income protection insurance schemes

For group income protection insurance schemes, we process limited health data, such as sickness reports, notifications of recovery or to what extent you are unfit for work. We receive these data from you, your employer, the working conditions service or the UWV (Employee Insurance Agency).

If we support you and your employer in reintegration, our reintegration staff can also process information about your limitations and capabilities, so that we can help you return to work in a responsible way.

Personal injury

In order to assess and handle a personal injury claim, we will process your health data. We may share your data with other parties, such as personal injury firms. Our employees will only process healthcare data they need to carry out their tasks.

Only the medical adviser is allowed to process your health data for the purpose of preparing medical advice. To this end, the medical adviser can request additional health data from you. The medical adviser will only collect health data from you from other sources with your explicit consent, if necessary with authorisation.

back to contents >

Are you dealing with a personal injury claim, for example? You will then receive a separate brochure containing an explanation of the use of your (health) data.

Individual disability or private and business accident insurance and travel insurance with accident cover
The medical adviser plays a central role in assessing your health in connection with the conclusion of an insurance policy or a claim for benefits due to disability or an accident. Only the medical adviser and the employees working under their responsibility may process your health data. If the medical adviser considers it necessary for the assessment of your application or for the assessment of your disability to request health data from others, such as your GP or treating specialist, he/she will always ask you for your prior consent. The authorisation with which you give this consent states which health data the medical adviser wishes to request and from whom.

By signing the authorisation, you give your consent. The medical adviser is responsible for retaining your health data. When processing health data, we comply with the Code of Conduct for the Processing of Personal Data by Insurers. When processing health data, the medical adviser complies with the Professional Code for Medical Advisers working in Private Insurance cases and/or Personal Injury cases.

Pension insurance
For group pension insurance, we do not process health data, except in the event of a claim for disability cover or if you change your mind about a previously made choice. For example, if you have chosen earlier not to participate in the Anw (Surviving Dependants Act) scheme with us, offered by your employer and at a later date wish to participate nonetheless, we may require health warranties from you.

Health insurance
For the application of your basic insurance, we do not need any health data from you in order to take out this insurance. We do not use risk selection for acceptance, as the basic insurance is subject to a statutory acceptance obligation. The government determines which cover is included in the basic insurance. If you apply for supplementary insurance with us, we may request health data from you in order to assess your application. In the case of supplementary insurance, we are free to decide whether or not to accept your application on the basis of risk selection.

As a health insurance company, we are allowed to process data about your health, to the extent necessary for the implementation of the basic insurance, the supplementary health insurance or Wlz (Long-Term Care Act) insurance. The processing of your health data takes place only within a specially separated unit (functional unit), under the responsibility of our medical adviser. This is a BIG-registered medical specialist. When processing health data, we comply with the Code of Conduct for the Processing of Personal Data by Health Insurers.

e. Criminal data
On contracting of non-life or individual income protection insurance, we may ask whether you or your co-insured parties have been in contact with the police or the judiciary in the past eight years. If you or your co-insured parties have a criminal record, we will assess whether that record affects your application. We do this in order to assess the risk if we accept you as a customer. You are required to answer the question truthfully. We may only use the stated criminal record for the assessment of the insurance application and to invoke inadequate compliance with the applicant's reporting obligation. We may also process criminal records in order to prevent fraud and abuse.
We process these data pursuant to Article 33 of the GDPR Implementing Act, the Code of Conduct for Processing of Personal Data by Insurers and the Financial Institutions Incident Warning System Protocol (PIFI). Criminal data (for example on your application form), will only be processed by employees who are authorised to do so.

f. Citizen service number (BSN)
In some cases, we also process your citizen service number (BSN). We only process your BSN if we have a legal basis for this.

g. Data on your contacts with us
We process data about the contact you have had with us in order to be able to see:
- What was the contact about (product, advice, an offer, a service call, message, complaint, information).
- When did the contact take place, with whom and how (via telephone, post, chat, our website, email, newsletter, app, adviser, web care team).

back to contents >

We use these data:
- To read or listen back what our previous contact with you was about. Then we can give you a more specific answer next time we have contact.

Recording and retaining telephone conversations
We record and retain chat and telephone conversations for, among other things:
- improving the quality of our services,
- training and coaching our employees,
- concluding and implementing insurance agreements,
- providing evidence and assessing (the content of) the communication (in the event of disputes of interpretation or disagreement about this),
- preventing and combating fraud and
- complying with statutory obligations.

We may also automatically convert recorded telephone conversations into text, which will then be used after analysis to improve the quality of our services.

We keep recorded calls no longer than is necessary in connection with the purpose for which the call is recorded. The retention period varies depending on the purpose for which a conversation was recorded. If a call has been recorded and is still available, in the event of a dispute about the content of the recorded call, you have the right to listen to the call or receive a transcription of it.

h. Company data
In the course of our business services we also process personal data like names of contact persons, shareholders or UBOs (ultimate beneficial owner) of a company. Under the Money Laundering and Terrorist Financing (Prevention) Act and sanction regulations, we must identify the UBOs of our business customers and suppliers. More information on this is available on the AFM website.

4. How do we obtain your data?

In most cases, we receive the data directly from you. In addition to the information we receive from you, we may also receive and process data from third parties, such as your employer, adviser, an authorised agent, a(nother) (re) insurer or other parties such as the Trade Register and the UBO Register of the Chamber of Commerce, Statistics Netherlands (CBS), the Central Information System Foundation (CIS), the National Vehicle and Driving Licence Registration Authority (RDW), the Credit Registration Office (BKR), the Land Registry, the Insolvency Register, the Personal Records Database (BRP), the Employee Insurance Agency (UWV), IDIN, EVR, government authorities (lists of government agencies, such as PEP and sanctions lists and occupational health and safety services, market research firms, data enrichment firms or credit reporting agencies.

We can also consult other (public) sources, such as public registers of The Dutch Central Bank (DNB) and the Dutch Authority for the Financial Markets (AFM), sources such as newspapers, the internet and your public social media profiles in order to trace or prevent fraud and abuse and to protect a.s.r.

You can also give a.s.r. permission to have data collected via the Ockto app, whereby we receive and process information from third parties such as for example the Tax and Customs Administration, UWV, Overheid.nl and mijnpensioenoverzicht.nl. In our processing register we record from which third parties (sources) we have received data if we know these sources.

Your visit to our websites and apps
We record information about your visit to our websites or apps, for example which pages you visited, when you logged in on the 'My platform' or your search queries. This allows us to better respond to your personal experience the next time you visit our website. These data we may also use for marketing purposes. We do this by, among other things, placing cookies. We also process your IP address in this context. As our websites or apps may place different cookies, we refer to the applicable cookie statements of the website or app that you visit/have

back to contents >

visited for information on the specific cookies used. If you visit one of our websites, you will generally find the cookie statement in the footer of the website.

5. Why do we process your data?

Purposes for the processing of personal data are:

a. The performance of our services

We use your personal data, among other things, to contact you in order to check whether you can become or remain a customer with us, to consult with you about the products or services that you purchase from us, to implement changes in your personal data or to provide you with (financial) insight and perspective for action via the platform 'Ik denk vooruit'
(I think ahead).

We may use your data to manage your products - or the products of your employer, such as absenteeism insurance policies - and to settle (expense) claims and complaints or to receive, pass on and have your order executed.

b. Reducing and assessing risks

We also use your personal data to reduce and assess risks, for example by:
- ensuring adequate security. Consider for example user names, passwords and control questions.
- conducting an internal quality investigation into the possible problems and risks and to assess whether legislation and regulations have been implemented correctly.
- knowing our customers (customer screening) and thereby ensuring that we remain a healthy company (risk management).
- performing customer screening not only before or at the start of a customer relationship, to determine whether we can accept you as a customer, but we must also do this during the relationship, to determine whether you can remain a customer.
- consulting various (public) sources as well as our Central Occurrences Database, our Incident Register (IVR) and the incident registers of the joint financial institutions (EVR) in accordance with the PIFI (see also paragraphs 3 and 4), both when you become a customer and while you are a customer (for example in the case of claim handling).
- making or commissioning (statistical and/or scientific) analyses and reports and delivering insights at aggregate level, for example in order to be able to better assess risks. Where possible, we erase the personal data that we do not need. And we may bundle data at a certain abstraction level (aggregate), encrypt (pseudonymise) or anonymise them.

c. Performing marketing activities

We are happy to keep you informed. For example through emails, newsletters, offers on our website or via social media. Or with personalised ads on apps and websites of other parties and social media. For this, too, we use your personal data.

We can do this by:
- looking at which a.s.r. products and services you are already using and which you are not. We do this by using cookies, for example. For more information on this, see the cookie statements on the specific websites of our brands and entities.
- collecting and analysing your choices and searches, for example when you visit our web pages or apps and open emails such as the newsletter. For example, you may be interested in participating in the a.s.r. Vitality programme or be interested in car insurance when you visit certain pages of our website.
- combining the data we have collected ourselves with personal data (for example an application for another financial product) and general data from other sources (for example Chamber of Commerce).

Would you rather not receive personal offers? Please let us know (see also 10.f. and 15).

back to contents >

d. Improving and innovating

We also use your personal data to improve our products and services and to tailor our range of products to your wishes and needs.

We do this by combining and analysing them. These analyses bring us new ideas in the context of innovation benefiting you, your contact with us and your products and thus to better solutions. Based on these analyses, we may for example:

- solve the cause of complaints, improve pages and forms on the website and speed up processes.
- measure how customers use our services and what the result is of a campaign. And, if necessary: improve things.
- develop new services.
- make or commission (statistical and/or scientific) analyses and reports and deliver insights at aggregate level, for example to be able to properly determine the prices of our products and services. Where possible, we remove the personal data that we do not need. And we may bundle data at a certain abstraction level (aggregate), encrypt (pseudonymise) or anonymise them.

e. Tracing fraud and abuse

We obtain the personal data that we process in connection with the tracing and control of fraud, abuse and improper use from various (public) sources (see also paragraph 4). We can also receive information in that regard from tipsters or witnesses. We can also gather information by conducting or arranging to conduct technical, tactical and personal investigations. We can deploy investigative agencies to conduct these investigations. If a personal investigation in connection with insurance is involved, we follow the rules of the Code of Conduct for Personal Investigations. In the detection and control of fraud, abuse and improper use, we also record personal data in our Central Occurrences Database, our own Incidents Register (IVR) and in that of the financial sector (EVR).

Central Occurrences Database

In order to protect the security and integrity of different entities and brands within ASR Nederland N.V., we use a Central Occurrences Database. In this database, (personal) data are saved that require our special attention in relation to certain occurrences. Data from the Central Occurrences Database are only accessible to our Security and Special Affairs departments, or to other employees authorised for that purpose.

EVR

With the aid of the joint registers of the financial sector (EVR), we can exchange data of entities and brands within ASR Nederland N.V. with other financial institutions or with external research agencies. We comply with the rules of the Insurers and Crime Protocol and the PIFI here. Organisations including the following are involved in the PIFI:

- the Dutch Association of Insurers,
- the Dutch Banking Association,
- the Mortgage Fraud Prevention Foundation,
- the Dutch Finance Houses' Association and
- the Association of Dutch Health Insurers.

IVR

In order to protect the security and integrity of the different entities and brands within ASR Nederland N.V., we use our own incidents register (IVR). In this database, (personal) data are saved that require our special attention in relation to certain incidents. Data from the incidents register are only accessible to our Security and Special Affairs departments, or to other employees authorised for that purpose.

If we record your data in the EVR or IVR registers in relation to fraud or other forms of insurance crime, we specifically inform you of this in advance (which data, why and for how long), unless this is not permitted or if this would harm the investigation, for example because the police ask us not to inform you in the interests of their investigation. If you disagree with the recording of this data, you can file an objection or ask us to correct or erase your data (see also paragraph 10). Please note that you can make a request to the CIS Foundation to view the EVR records (an overview of records) relating to you. The CIS Foundation uses its own privacy and user regulations for that purpose. These can be viewed on the website of the CIS Foundation. A request to view data can be sent to us, insofar as this concerns records that we have entered in the Central Occurrences Database, the EVR or the IVR.

More information is available in the Insurers Personal Data Processing Code of Conduct (GVPV) and the PIFI.

back to contents >

f. Business transactions and business operations
We may process your personal data if this is necessary in connection with business transactions and the business operations of a.s.r. For example, contemplated or actual mergers, acquisitions, full or partial transfer of assets (such as mortgage loan receivables), financing, contemplated or actual legal proceedings, bankruptcy or restructuring of all or part of the business activities.

6. What is the legal basis for using your personal data?

We process your personal data on the basis of one of the following statutory bases:

a) You have given your consent.
When we process your personal data on the basis of your consent, you may withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
b) The processing is necessary for the performance of the agreement.
c) The processing is necessary to meet a statutory obligation.
Financial service providers are subject to various legal obligations. For example, we are obliged to identify you when you become our customer (identification requirement) and in certain cases we are obliged to provide data to the Tax and Customs Administration (information reporting). As a result of these obligations, we need to request these data from you. If you do not provide these data, this may have consequences for you: if we cannot identify you or if we do not receive data, or inaccurate data, about your criminal record, we cannot enter into an agreement with you. If an agreement with you has already been concluded, we may terminate it if the information you provided is incorrect.
d) The processing is necessary to promote a justified interest, for example when we conduct an investigation into possible fraud or when we process personal data in the context of business transactions and business operations. In that case we will weigh up our or a third party's justified interest and yours. This weighing of interests will be recorded and we will inform you as much as possible.

7. How do we secure your data?

We handle your personal data with due care. We have put in place technical and organisational measures to guarantee an adequate protection level and to protect your personal data against loss or unlawful processing. We pay great attention to the optimal security of our systems in which personal data are stored. For example, measures to use our websites and IT systems safely and avoid abuse. But also protection of physical spaces where personal data are stored. We monitor the security of our data traffic 24 hours a day. We have an information security policy in place and arrange training programmes of our staff in the area of personal data protection.

Only authorised employees, who should have access to your data, can view and process your data. All our employees have taken an oath or have made a solemn affirmation in which they have promised or stated that they will comply with the legislation and regulations and codes of conduct and that they will act ethically. In certain cases (e.g. access to sensitive personal data), employees must first sign an additional confidentiality agreement before being granted access.

8. How long do we retain your data?

We do not store your personal data longer than necessary. In certain cases the law provides how long we may or must store data. In other cases, we have determined on the basis of legislation and regulations how long we need your data. We have drawn up an extensive retention period policy for this.

Policy/customer files for example are stored for at least 7 years after the relationship with a.s.r. has ended.
For more information on the specific retention periods, please contact us.

back to contents >

9. 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 ASR Nederland N.V.

a. Within ASR Nederland N.V.

Are you a customer of one of the entities or brands that come under ASR Nederland N.V.? In that case we may exchange your personal data with one of the other entities or brands of ASR Nederland N.V. This also applies for entities or brands that are not named in this privacy statement, but that are headed by ASR Nederland N.V. We do this, for example, for administrative reasons, to ensure a responsible acceptance policy or to prevent and combat fraud. In addition, we exchange personal data between the various departments of ASR Nederland N.V., for example for the processing of your application or to obtain an overview of the products and services supplied to you. This allows us to provide you with a better service; for example, you only have to pass on a change of address once.

You may receive offers for other products of the entities and brands that come under ASR Nederland N.V. If you do not want to receive any offers for other products, you can indicate this. If you have an adviser, you will usually only receive messages from us in consultation with your adviser (see also c.).
Your personal data are stored in a.s.r.'s central customer administration. This is done for internal administrative purposes, including the matching of your data. This means that we check whether the same data about you are used in the various business units. It is important to check whether we have the right information about you.
By matching data, we can work more efficiently and provide you with a better service.

b. The authorities

Sometimes we are required by law to pass on certain personal data to the authorities. These may include the Tax and Customs Administration, the UWV, the police, the judiciary, the UBO Register of the Chamber of Commerce or supervisory authorities such as the Dutch Central Bank (DNB), the Netherlands Authority for the Financial Markets (AFM) and the Dutch Data Protection Authority (AP) and the Authority for Consumers and Markets (ACM).

c. Adviser/insurance agent

If statutorily permitted, we may exchange the personal data necessary for the services with your adviser/insurance agent. We do this for as long as you have an agreement with us. Sometimes we will need your consent for this. Your agent is responsible for the processing of your personal data. If your employer has engaged an agent or adviser, we will also exchange personal data with them. For the purpose of activating the 'My platform', we may obtain your email address from your adviser/agent.

d. Other insurer(s)

As a (health) insurer, we sometimes exchange information in order to recover damage or costs that we have paid, for example from your travel insurer if it also offers cover in addition to your basic or supplementary insurance, or from the liability insurer of another person who caused the damage or costs.

e. Service providers and companies we work together with

We engage other companies to perform services for us relating to our services. For example a debt-collection agency, a loss adjustment firm, a civil-law notary, a repairer, a re-integration agency, an occupational health and safety service or a reinsurer. We can also share personal data with a lawyer or representative. We also share your data with the Emergency Centre as the executor of (breakdown) assistance. If you have taken out legal expenses insurance with a.s.r., we will share your data with DAS as the provider of the legal assistance. If you have taken out a mortgage with us, we can share your personal data with the the Credit Registration Office (BKR), the National Mortgage Guarantee (NHG) scheme and the Homeowner's Guarantee Fund Foundation (WEW). When you take out a health insurance policy with a.s.r., we will share your personal data, but no special category personal data (such as health data), with Zorgdomein, to promote referral flows by healthcare providers to other healthcare providers. With all parties, we lay down agreements to safe- guard your privacy.

back to contents >

We may also outsource the processing of personal data for maintenance and support functions to third parties, for example (IT) service providers. In most cases, these (IT) service providers are to be considered as processors because they do not have independent control of the personal data that a.s.r. makes available to the IT service provider in the context of the services. In these situations ASR Nederland N.V. remains responsible for the careful processing of your personal data.

f. Parties involved in business transactions and business operations
In connection with business transactions and business operations, as explained under 5.f., we may share personal data with third parties. This may include parties that are themselves involved in the business transactions and business operations, such as (potential) buyers of assets, an opposing counter-party in legal proceedings or financiers in a business transaction. But it may also include professional advisors to those parties or, for example, a bailiff, if this is necessary for the business transaction or business operations.

g. Central Information System (Foundation) (CIS)
For a responsible acceptance and risk policy in order to detect or prevent fraud, we record your personal data in and consult the Central Information System of the CIS Foundation. We record matters including your claims in this register, complying with the rules of the CIS user protocol, the Insurers and Crime Protocol and the PIFI. Subject to strict conditions, we can exchange information with other insurers that are affiliated with the CIS Foundation. We consult this register in the acceptance process and in the event of any claims handling. More information on this and the privacy regulations of the CIS Foundation are available on the CIS Foundation website.

h. External Reference Index (EVR)
Financial institutions may record in an Incidents Register the conduct of persons or legal entities that has led or may lead to prejudicing financial institutions. An External Reference Index is linked to this Incidents Register. This External Reference Index only contains referral data (e.g. a name and date of birth or Chamber of Commerce number) to the Incidents Register that may be included under strict conditions in accordance with the Protocol on the Financial Institutions Incident Warning System Protocol (PIFI). Every financial institution that is affiliated to one of the participating industry associations has access to (part of) the External Reference Index.

i. Third parties outside the European Economic Area (EEA)
Your data are mostly processed within the European Economic Area (EEA). If we share data with parties based in a country outside the EEA or if personal data are processed outside the EEA, we ensure that your personal data remains adequately protected. In doing so, we for example make use of the Standard Contractual Clauses (European Model Clauses). We put in place clear agreements with parties, to ensure that the processing takes place in accordance with European legislation.

Your personal data will not be sold.

back to contents >

10. What are your rights?

a. Inspecting or correcting data (inspection and rectification)
You have the right to ask us what personal data we process about you and to have incorrect data adjusted. We will ask verification questions or ask you for a copy of your proof of identity* to identify yourself.

After identification, you will receive our response within four weeks.
In certain cases we may choose not to give you any data about your health, for example if we consider it wiser that your GP provides an explanation. In such cases we will inform you about the way in which the information can be shared or requested.

**Proof of identity*
When you provide a copy of your ID, you need to make your passport photo and citizen service number (BSN) invisible. We also recommend that you state on the copy that this copy serves to exercise your rights relating to your personal data.

b. Having your data removed and the right to 'be forgotten'
In certain 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 for the purposes for which they were collected or have been processed in other ways;
- you have withdrawn your consent to process them;
- you file a well-founded objection against the processing;
- your personal data have been unlawfully processed by us;
- there is a statutory obligation to delete the personal data;
- the personal data are related to your child and were collected in connection with a direct offer for 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 delete your data, if your request is not based on one of the above grounds, or (i) in order to exercise the right to freedom of speech and information; (ii) to satisfy a statutory obligation; or (iii) to institute, exercise or substantiate a claim. If we do not honour your request to have your personal data deleted, we will inform you about the reasons why we will not comply with your request.

c. Restriction on the processing
If you are of the opinion that we process your personal data unlawfully, you may request that the processing be restricted. 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 are entitled to a copy of the personal data you have provided to us for the performance of an agreement you have concluded with us or if you have given us permission to use them. This only concerns personal data that we received from you yourself, not data we received from third parties. The purpose of this right is to enable you to easily transfer this data to another party.

e. The right to file an objection
You may at any time object against the processing of your personal data that takes place on the basis of our justified interest or the justified interest of a third party. In that case we will no longer process your data unless there are urgent, justified grounds for the processing that bear more weight, or which are related to instituting, exercising or substantiating a claim.

back to contents >

f. Unsubscribing from personal offers

You have the right to unsubscribe from newsletters or personal offers via various channels (for example email, phone and mail) for our insurance and other (financial) services. In commercial offers we always point to the possibility to unsubscribe. Our staff may call you for commercial purposes. If you receive such calls from us, you can indicate during the telephone conversation that you no longer wish to be called. You can also contact us yourself and let us know that you no longer wish to be called. When we make profiles to make personal offers for products and services that match your personal preferences and interests, you can object at any time to the use of your personal data for this purpose.

See paragraph 15 for information on how you can make use of your rights.

11. Email and social media (chat, WhatsApp, Facebook)

a. Email

If required, before we communicate with you via email (digital communication), we will ask your permission for this, unless you have already given us permission.

If you have a pension insurance with us through your employer, we will not ask you for permission to communicate with you via email, because the legislator has chosen digital communication as the starting point for pension insurance.

b. Social media

You can opt to chat with us on our website or contact us via our social media pages such as Facebook, LinkedIn and Twitter or via WhatsApp. If you approach us via one of these channels, we will retain the data you provide to us via these channels in a secured environment. To respond to personal questions in your social media message, we will ask you in a personal message (direct message or email) to share your contact details with us. This allows us to check whether we are communicating with the right person.

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 deal with the personal data provided by you. Please note that many social media platforms are established outside the European Union and store data outside the European Union. The European Union's privacy legislation usually doesn't apply in that case. We would advise you to consult the privacy statement of these social media channels for more information about the way in which they process your personal data.

back to contents >

12. Profiling and automated decision-making

Profiling
We make profiles of our customers on the basis of the data we collect with the purpose of analysing these data and thus, among other things, managing risks, making connections, and obtaining insight into (future) actions and preferences. We can then anticipate these. For example, by using these data to estimate the contribution or to send customers targeted advertisements/information. When we do so, we comply with legislation and regulations. This means, among other things, that we ask your permission beforehand if this is statutorily required. For example in the event of profiling based on sensitive personal data.

Automated decision-making
In particular cases we may use an automated process to assess an insurance application or a claim notification. This enables us to offer you a faster and better service . If you apply for an insurance, the data you supply will automatically be assessed in accordance with our acceptance criteria. This allows us to make a risk assessment of your application. In the event of a claim notification, your supplied data will automatically be assessed in accordance with our damage assessment criteria. This allows us to check whether a damage is covered. In both processes we will verify the supplied and available data. The decision about your application or claim notification will be based on the data you provide, risk- and fraud indicators and data from (public) sources such as the CIS database. After that, the application can be automatically accepted or the claim can automatically be paid. However, in case of a deviation in the regular process, for example if the application or claim is rejected your application or claim notification will be assessed by an a.s.r. employee. You have the right to obtain human intervention on the part of a.s.r., to express your point of view on the decision made and to contest that decision.

If you apply for basic or additional health insurance your data will be processed through an automated process. Data will be retrieved from the electronic application form that you have filled out. Additionally, authorization requests and declarations are screened to judge whether the application is covered within the insurance. Assessment of these criteria can be performed through an automated process. The outcome of the review of the declaration, either approval or rejection, will be communicated to you. You have the right to obtain human intervention on the part of a.s.r., to express your point of view on the decision made and to contest that decision.

13. Supervision

A number of bodies monitor how we process personal data:
- The Dutch Data Protection Authority (AP; supervises compliance with the GDPR (General Data Protection Regulation).
- The Dutch Authority for Consumers & Markets (ACM); supervises compliance with the Telecommunications Act (including cookies and direct marketing).
- The Dutch Central Bank (DNB) and the Dutch Authority for the Financial Markets (AFM); generally supervise the financial sector (including customer's interest).
- The Data Protection Officer of ASR Nederland N.V. and the Data Protection Officer of Aegon for the Aegon entities referred to in this privacy statement (see also paragraph 15).

14. Amendment of the privacy statement

Privacy legislation is not static. Therefore we can amend this privacy statement in order to keep it up-to-date. We will do so if there are new developments, for example if there are changes in our business activities or in the law or case law. Therefore you are advised to regularly check this privacy statement when visiting one of our websites. In case of a material change to this privacy notice, a notification will be provided (for example through our website).

back to contents >

15. Any questions or complaints?

Any questions?
If you have any questions, for instance about this privacy statement, of if you wish to make use of your rights, you can contact us at any time via one of the channels available for that purpose. If you have questions concerning one of the Aegon entities referred to in this statement, please see the contact details on the Customer Service page of the Aegon website. You can use the form on the Aegon website to exercise your rights at Aegon.

You can contact the Data Protection Officer of ASR Nederland N.V. by sending an email to privacy@asr.nl or a letter to:

Data Protection Officer.
Compliance Department
a.s.r.
PO Box 2072
3500 HB Utrecht

You can contact the Data Protection Officer for the Aegon entities referred to in this privacy statement by sending an email to fg@aegon.nl.

Complaints
If you have any complaints about privacy, you can contact us using the complaints form on our website.

If you have any complaints about privacy relating to the Aegon entities referred to in this privacy statement, please use the complaints form on the Aegon website.

You can also submit a complaint to the Dutch Data Protection Authority (AP) at www.autoriteitpersoonsgegevens.nl (Tel. +31 88 1805250).

Privacy statement most recently updated 2 October 2023.

back to contents >

a.s.r.
Archimedeslaan 10
3584 BA Utrecht
www.asr.nl

ASR Nederland N.V., Chamber of Commerce 30070695 Utrecht

50436EN_0923