Privacy Statement
ASR Nederland N.V.

December 2024

Contents

1. When does this privacy statement apply?

When you purchase a product or service from us, we need data from you to ensure we can deliver that product or service to you. You can trust us to handle your data with due care. In doing so, we comply with applicable legislation and regulations, the Code of Conduct on Processing Personal Data for Insurers and the Code of Conduct on Processing Personal Data for Healthcare Insurers.

This privacy statement applies to all personal data that ASR Nederland N.V. and its business units process from you. This may be the case if you are a customer, or if you are not a customer but have contacted us, if your employer is a customer and you are a participant in its agreement or if you are a beneficiary, aggrieved party or guarantor. In our business services, we may process data of contact persons, shareholders, or UBOs of a company. UBOs are natural persons who ultimately own or control a company or organisation.

When you visit our websites or use our apps, such as your a.s.r. account, we process some data from you to provide and technically manage the functionalities of these online services. We may also show you personalised ads, if you gave your consent. The processing of your personal data depends on your settings. See our cookie statement . When we mention a.s.r. in this privacy statement, we mean ASR Nederland N.V. and the a.s.r. labelled business units.[1]

Some business units have their own privacy statements. These include ASR Real Estate B.V., ASR Real Estate Investment Partners and the Raad van Doen. For more information, see:
- https://asrrealestate.nl/privacyverklaring
- https://asrinvestmentpartners.nl/privacy-statement
- https://asr.nl/klantpanel

2. Who is responsible for your personal data?

A controller determines how and why personal data are processed. The controller determines the purposes and means of processing personal data and is the point of contact for you as a data subject.

ASR Nederland N.V., with a number of its business units, is jointly responsible for processing your personal data. Mutual agreements have been reached on the division of our responsibilities. These are the following parties: ASR Schadeverzekering N.V., ASR Levensverzekering N.V., Aegon Levensverzekering N.V., Aegon Spaarkas N.V., ASR Basis Ziektekostenverzekeringen N.V., ASR Aanvullende Ziektekostenverzekeringen N.V., ASR Vermogensbeheer N.V., ASR Real Estate B.V., ASR Wlz Uitvoerder B.V., ASR Premiepensioeninstelling N.V., Aegon Cappital B.V., ASR Vooruit B.V., Aegon Hypotheken B.V., Loyalis and a.s.r. Vitality.

1 ASR Levensverzekering N.V., ASR Basis Ziektekostenverzekeringen N.V., ASR Aanvullende Ziektekosten verzekeringen N.V., ASR Schadeverzekering N.V., ASR Vermogensbeheer N.V., ASR Vitaliteit en Preventieve Diensten B.V., ASR Vooruit B.V., ASR Premiepensioeninstelling N.V., ASR Reïntegratie B.V., Advies van a.s.r.
But also: Aegon Hypotheken B.V., Aegon Levensverzekering N.V., Aegon Cappital B.V., Aegon Bemiddeling B.V., Aegon Administratie B.V., Aegon Administratieve Dienstverlening B.V., Aegon Spaarkas N.V. and Loyalis.
The privacy statement also applies to the labels no longer operated by a.s.r., to the extent that a.s.r. still processes personal data in that context, including: Ardanta, Europeesche Verzekeringen, ZZP Pensioen, Axent, De Eendragt and Generali Nederland.

It has been agreed with the above parties that ASR Nederland N.V. will be your first point of contact.
Visiting address:
Archimedes Avenue 10
3584 BA Utrecht
Postal address:
PO Box 2072
3500 HB Utrecht
- Facebook
- X
Telephone: +31 (0) 30 257 9111

a.s.r. has an internal Data Protection Officer (email address: anl.compliance.fg@asr.nl) This officer ensures that the processing of personal data within a.s.r. complies with the General Data Protection Regulation (AVG).

3. What personal data do we process?

When you or your employer apply for insurance or another (financial) product or service from a.s.r. or request information, we ask for your personal data. What data we process from you depends on which product or service you purchase.

a. **Name and address details**
Name and address details and contact details such as email addresses and phone numbers. We use this data to send you information, contact you and execute (insurance) agreements.

b. **Financial data**
We use your bank account number to make payments and collect amounts due (premium, fee, periodic deposit or interest). In addition, we may have your income details if this is necessary for one or more of our financial products.

c. **Additional data**
For some products or services, we still need additional information, such as dates of birth, gender, occupation or licence plate number to determine the premium and take out the insurance.

d. **Health data**
To accept or perform our insurance and other (financial) services, we need information about your health in certain cases. Sometimes we need information from your physician. If we need data from your physician, we will always ask for your prior consent. Health data are shared only with the medical service.

Health insurance
To apply for your basic insurance, we do not need any health data from you to take out this insurance. We do not use risk selection for acceptance, as basic insurance is subject to a statutory duty to accept. We use your personal data to check whether you are required to be insured for basic insurance. The government determines which cover is included in the basic insurance. If you apply for supplementary insurance with us, however, we may request health data from you to assess your application. For supplementary insurance, we are free to accept or not accept your application based on risk selection.

As a health insurer, we are allowed to process data about your health to the extent necessary for the implementation of the basic health insurance, the supplementary health insurance or the Wlz insurance. The processing of your health data takes place only within a special separated unit (functional unit), under the responsibility of our medical advisor. That 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
When taking out non-life or individual income insurance, we may ask you about your criminal record, or that of your co-insured person(s). We will then assess whether this criminal record will affect your application. Only your criminal record in the eight years preceding the application for insurance is relevant in this context. We do this to assess how high the risk is if we accept you as a customer.

We may also process criminal data to prevent and deter fraud and abuse. We adhere to the Insurers and Crime Protocol and the Protocol on the Warning System for Financial Institutions (PIFI) when processing criminal data.

f. Citizen service number (BSN)
In some cases, we also process your citizen service number (BSN). We will only process your BSN if we are required to do so by legislation.

4. How do we get your data?

We may receive your personal data in various ways.

Data we receive from you
In most cases, we get the data directly from you. When you:
- conclude a product with us or purchase a service from us.
- contact us via the website (application form or chat) or fill in the contact form.

Data we receive from a third party
We may also receive your data through a third party. For example, when:
- your advisor, broker or employer requests a product or quotation from us for you.
- your employer has insured your pension or absenteeism with us.

Data we obtain from external sources
To assess your application or (claim) report, we collect and process personal data from external sources. The external sources can be public sources such as the vehicle registration register, Trade Register, Land Registry, Bureau Kredietregistratie (BKR) and credit reference agencies. Among other things, we do this to:
- verify the data you entered.
- be able to prepare data for you in advance.
- to assess whether there are risks of fraud, default or claims.

In addition, as administrator of pensions and health insurance, a.s.r. has access to the Basic Registration of Persons (BRP). And we receive monthly disability data from pension members via the UWV's Disability Benefit Status (SUAG) product.

5. Why do we process your data?

Purposes for the processing of personal data are:

a. The performance of our services
Among other things, we need your personal data if you want to become a customer with us to make an offer or assess your application. If you are a customer, to provide information and advice on the products or services you purchase from us.

We use your data to manage and perform the agreements and services such as handling your claims, declarations, damages and complaints or receiving, transmitting and fulfilling your order.

If you do not want to share the data we request from you, we cannot enter into an agreement with you.

b. To comply with legislation and regulations

There are laws that require us to request, retain and sometimes provide your personal data to other parties.

- We need to establish your identity under tax and supervisory legislation.
- The Sanctions Act and the Prevention of Money Laundering and Terrorist Financing Act require us to establish and verify your identity. We also need to check whether you appear on national and international risk and sanctions lists.
- Under the Financial Supervision Act, we are required to prepare a risk profile.
- If you apply for a mortgage or loan, we are obliged to check your creditworthiness with the BKR. And we report certain arrears to the BKR.
- We are also required to disclose your personal data to a government agency, a regulator, a judge or other financial institutions. For example, the Tax Authority, AP, AFM, DNB or ACM, the Pension Register Foundation (www.mijnpensioenoverzicht.nl) or an investigative body such as police and the Fiscal Intelligence and Investigation Service (FIOD).
- We collect data about your property, such as your energy label, energy performance and any climate risk to meet our Environmental, Social, and Governance (ESG) reporting obligations. This data is obtained from public sources and then aggregated in our reports.

c. Conducting customer due diligence

To prevent money laundering and terrorist financing, we are required by law to know our customers and not to enter into relationships with individuals who could damage trust in the financial sector. Therefore, before entering into a customer relationship with you, we need to see if we can accept you as a customer. That means we can ask you to identify yourself and investigate if you have any assets, make an unusual repayment on your mortgage or if there is an unusual transaction on your account. In addition, we must report unusual transactions to the competent investigating authorities and regulators, such as FIU-the Netherlands. We also have to check whether you appear on national and international risk and sanctions lists. And during our customer relationship, we need to keep examining whether we can keep you as a customer.

After completing the customer survey, you will be assigned a risk profile. The risk profile determines how often and to what extent you should be monitored. Depending on what we find during our periodic monitoring, your risk profile may change. So your risk profile is not fixed forever.

d. Conducting marketing activities

If you are a customer with us, we would like to inform you about our other products and services. For example, by emails, or offers on our website or through social media. We also use your personal data for this purpose.

We do this to:

- send you general newsletters with information and offers on our products and services via your a.s.r. account.
- be able to make you offers that respond to your personal situation. For this, we look at which a.s.r. products and services you already use and which you do not. We do this by using cookies, for example. For more information on this, see the cookie statement on specific websites and our apps.
- show you more targeted ads on our websites or on websites of other companies. We collect and analyse your choices and search queries when you visit our web pages or apps and open emails, we do this through the use of cookies. See the cookie statement.

Do you prefer not to receive personalised offers? Let us know (see further under 11f and 16).

e. Improving and innovating

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

We do this by combining and analysing personal data (or having it analysed) and using it for innovations. This is how we come up with new ideas in the context of innovations for the benefit of yourself, your contact with us and your products or our services and thus to better solutions. This way, we can:

- resolve the cause of complaints, improve pages and forms on the website, and improve and speed up processes.
- measure how customers use our services and the results of a campaign. And if necessary: improve our services.
- develop new applications, products and services, including developing (including testing) Artificial Intelligence (AI) applications.
- as part of the management, including testing, of our (new) (administration) systems/applications, ensure that they function properly and in so doing guarantee the continuity of our services.
- create (statistical and/or scientific) analyses and reports (or have them created) and provide insights at an aggregated level, for example to properly price our products and services.
- recording and listening back to telephone conversations for training- and coaching purposes

When we perform analyses, we use your data anonymised or pseudonymised as much as possible. This means the data is no longer directly traceable to you. And we take appropriate measures to secure your personal data. We also ensure that only a small group has access to the analyses.

f. Preventing and detecting fraud and abuse

We obtain the personal data we process in the context of detecting and combating fraud, abuse and improper use from you and from various (public) sources (see below under 4). We may also receive information from tip-offs or witnesses in this context. We may additionally gather information by, for example, carrying out or commissioning technical, tactical and personal investigations. In conducting these surveys, we may use research agencies.

In detecting and combating fraud, abuse and improper use, we also record personal data in our Central Events Records, our own Incident Register (IVR) and those of the financial sector (EVR).

Central Events Administration (Centrale Gebeurtenissenadministratie)

To monitor the security and integrity of a.s.r., we use a Central Events Administration. This database stores (personal) data in respect of certain events, which require our special attention. Data from the Central Events Administration can only be accessed by employees authorised to do so.

EVR

The Financial Industry Joint Registers (EVR) allow us to exchange data within a.s.r., with other financial institutions or with external research agencies. In doing so, we adhere to the Insurers and Crime Protocol and the Protocol on the Warning System for Financial Institutions (PIFI). Those involved in the PIFI include:

- the Dutch Association of Insurers,
- the Dutch Banking Association,
- the Foundation for the Combating of Mortgage Fraud (SFH),
- the Association of Finance Companies in the Netherlands and
- Health Insurers Netherlands.

IVR

To monitor the safety and integrity of a.s.r., we use our own incident register (IVR). This database stores (personal) data in respect of certain incidents that require our special attention. Data from this incident register can only be accessed by employees authorised to do so.

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). Except if this is not allowed or the investigation is harmed as a result, for example because the police ask us not to inform you in the interest of their investigation. Do you disagree with the recording of these data? Then you can object to this or ask for your data to be corrected or deleted (see below under 11). Please note that to access the registrations relating to you in EVR (an overview of registrations) you can make a request to the Foundation Central Information System (Stichting CIS).

g. Business operations
We may process your personal data if this is necessary in the context of a.s.r.'s business operations. Examples include mergers, acquisitions, full or partial transfer of assets (such as claims from mortgage loans), financing, contemplated or actual legal proceedings, bankruptcy or restructuring of all or part of the business activities.

6. Why may we use your personal data?

We may use your personal data because there is a legal basis. These are:
- you gave your consent.
  If we process your personal data based on your consent, you can withdraw your consent at any time. The withdrawal of consent does not affect the lawfulness of the processing prior to its withdrawal.
- the processing is necessary for the performance of the agreement.
  We need your data to enter into an insurance contract, but also if you are a beneficiary or the insured. We also need your personal data to pay compensation.
- the processing is necessary to comply with a legal obligation.
  Financial companies are subject to various legal obligations. For example, we are required to carry out a customer due diligence pursuant to the Sanctions Act or the Prevention of Money Laundering and Financing of Terrorism Act. To do this, we need certain personal data.
- the processing is necessary to pursue a legitimate interest.

We process your personal data, for example, to ensure the security and reliability of our business and the financial sector. We therefore want to prevent, investigate and combat (attempted) criminal or impermissible behaviour directed against the financial sector, our clients and a.s.r. itself and its employees. There is a legitimate interest for a.s.r. to take on only trustworthy customers. This legitimate interest also exists for processing your personal data in marketing activities.

In doing so, a.s.r. always carefully weighs up all interests to assess whether there is a legitimate interest: of your interest, that of others and that of a.s.r. When assessing, we weigh whether there are other ways to achieve the same objective or whether we need less data.

7. 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 secure your personal data against loss or unlawful processing. We take great care to ensure optimal security of our systems in which personal data are processed. Consider, for example, measures to keep our websites and IT systems secure and prevent misuse. But also protection of physical spaces where personal data are stored. We monitor the security of our data traffic 24/7. We have an Information Security Policy and provide training for our employees on personal data protection.

Only authorised employees, who must have access to your data, can view and process your data. All our employees are bound to confidentiality and must not disclose your personal data unlawfully or unnecessarily.

8. How long do we keep your data?

We do not keep your personal data for longer than necessary. In some cases, the law prescribes how long we may or must keep data. In other cases, we determine how long we need your data based on legislation and regulations. We have drafted a comprehensive Data Retention Policy for this purpose.

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 specific retention periods, please contact us.

9. Who do we share your data with?

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

a. Within a.s.r.
Are you a customer of a.s.r.? If so, we may exchange your personal data with one of the other business units. We only exchange personal data within a.s.r. if we have a legitimate purpose for doing so. Such as:
- for responsible underwriting and to prevent fraud, money laundering and terrorist financing.
- to answer your questions or inspection requests about products and services of the various a.s.r. units.
- to better assess risks and premiums.
- to provide you with a good and efficient service.
- to ensure the quality of your personal data.
- for research and innovation.
- for internal (management) reporting.

b. Government and regulators
Sometimes we are statutorily required to pass on certain personal data to the authorities. These include the Tax and Customs Administration, the Employee Insurance Agency (UWV), Sociale Verzekeringsbank (SVB), CAK, Ministry of Health, Welfare and Sport (Centrum Indicatiestelling Zorg (CIZ), Zorginstituut), Board of B&W, Police/Judicial authorities, the Chamber of Commerce for the purposes of the UBO register or supervisors such as De Nederlandsche Bank (DNB), the Netherlands Authority for the Financial Markets (AFM), the Personal Data Authority (AP), Dutch Healthcare Authority (NZa) and the Consumer Authority & Markt (ACM).

c. Advisor, intermediary and authorised underwriting agent
When an advisor/intermediary or an authorised underwriting agent takes out a product with us for you or reports a claim to us, we exchange personal data with your intermediary. We will do this for as long as you have an agreement with us. Sometimes we need your permission to do so. Your intermediary is solely responsible for processing your personal data. If your employer has used an intermediary or advisor, we will also exchange personal data with them. For the purpose of activating your a.s.r. account, we may receive your email address from your advisor/intermediary.

d. Other insurer(s) and reinsurers
As a (health) insurer, we sometimes exchange data to recover damage or costs that we have reimbursed, for example from your travel insurer if it also provides cover in addition to your basic or supplementary insurance, or from the liability insurer of another person, who caused the damage or costs. As a pension administrator, we also exchange data to perform a value transfer. Some major risks we do not want to or are unable to bear ourselves, these are therefore placed with reinsurers. This reinsurer requires data for its insurance.

e. Companies we (need to) work with

We engage other companies to perform services for us that are related to our services. These include, for example, a debt collection agency, a firm of loss adjusters, a notary, a recovery agency, a reintegration agency an occupational health and safety service or an on-call service for death notifications. We may also share your personal data with your lawyer or fiduciary, accountant, curator and administrator. We also share your data with the Emergency Centre as the executor of (breakdown) assistance. If you have taken out legal aid insurance with a.s.r., we share your details with DAS as the executor of legal aid.

If you have taken out a mortgage with National Mortgage Guarantee (NHG) with us, we share your personal data with Stichting Waarborgfonds Eigen Woningen (WEW) for guaranteeing the NHG. Furthermore, if you have taken out a mortgage with us, we may share your personal data with the Bureau Kredietregistratie (BKR), e.g. in case of (persistent) payment arrears. When you have taken out health insurance with a.s.r., we share your personal data with Zorgdomein, VECOZO, Vektis, care offices and healthcare providers. We record agreements with all parties to ensure your privacy.

a.s.r. also provides personal data to the Dutch Association of Insurers. The Dutch Association of Insurers supports a.s.r. and the industry for the purpose of statistical research in risk and claims management. Survey results are always aggregated and not targeted at you.

The service providers listed above are themselves responsible for ensuring that they process your personal data in accordance with the law.

Outsourcing

We may outsource the processing of personal data to third parties for maintenance and support functions, e.g. (IT) service providers. These (IT) service providers are in most cases considered processors, because they do not have independent control over the personal data, which a.s.r. makes available to the IT provider in the context of the provision of services. a.s.r. remains responsible for the careful processing of your personal data in these situations.

f. Parties involved in the business operations

In connection with a.s.r.'s business operations, as explained under 5.e., we may share personal data with third parties. These may include parties that are themselves involved in the operations, such as (potential) buyers of assets, a counterparty 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 it is necessary for the business transaction or business operations.

g. External fraud registers

For a responsible underwriting and risk policy and to detect or prevent fraud, we record your personal data in and consult the Central Information System of the Foundation Central Information System (Stichting CIS). In this register, we record, for example, your claims. In doing so, we adhere to the rules of the CIS User Protocol and the Insurers and Crime Protocol and the Protocol on the Warning System for Financial Institutions (PIFI). With insurers affiliated to the Foundation Central Information System, we can, under strict conditions, exchange information. We consult this register in the acceptance process and in the event of a claim notification. You can find more information on this and on the Foundation Central Information System privacy regulations on the Foundation Central Information System website.

In addition, we may request data relating to you from the Foundation for the Combating of Mortgage Fraud (SFH) if you wish to take out a mortgage with us. SFH has a database that lists everyone who has committed mortgage fraud in the past.

h. 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 will ensure that the protection of your personal data remains sufficiently safeguarded. We then use, for example, the Standard Contractual Clauses (European model contract provisions). We make clear agreements with parties so that processing takes place in accordance with European legislation.

Your personal data will not be resold.

10. Additional information Vitality

Special personal data
When you participate in the a.s.r. Vitality programme, we process your data. We do this to help you get a healthier lifestyle. For this, we also use health data. Among other things, we process these data when paying out rewards, when you link a tracker to our app, when you have an a.s.r. Vitality Health Check and when you complete one of the questionnaires. This includes the following data: (sports) activities, lifestyle habits, eating habits, blood pressure, heart rate, cholesterol, BMI & waist circumference, your Vitality status and whether or not you smoke and/or used to smoke.

Sharing personal data within a.s.r.
Vitality may exchange your personal data with one of the other entities of a.s.r. to establish whether you have insurance. This is a condition for being a member of a.s.r. Vitality. Your Vitality status is shared with other entities only when necessary for the payment of the insurance cashback. The special personal data which a.s.r. Vitality possesses are not shared with other entities. These data are thus never used for the acceptance of an insurance application, the determination of the amount of the insurance premium or access to care or the assessment of a claim.

Sharing data with third parties
When you link an app (such as Apple Health or Samsung Health) or an activity tracker (such as an Apple Watch or a Fitbit) to the a.s.r. Vitality app we receive information about your (sports) activities. We use these data to award points for your performance.

Using an app or activity tracker is your own responsibility. This privacy statement does not apply to how these apps or activity trackers handle the data provided by you. Please note that many suppliers of these apps or activity trackers are based outside the European Union and store data outside the European Union. As a result, other privacy legislation than the GDPR may apply. We encourage you to consult the privacy statement of these suppliers for more information on how they process your data and the rights you have.

Profiling
Based on your app usage, registered activities, rewards claimed, status, age, gender and public or purchased data, we create a user profile. This includes whether you have completed a questionnaire or a health check. In doing so, we only look at whether you filled it out and therefore not at the answers or the outcome. We use your user profile to better help you take more exercise, or continue to exercise, offering a personalised experience. For example, based on your profile, you can get different notifications, rewards in a different order or see these specially highlighted, or get specific events highlighted. The user profile does not affect which rewards you are entitled to, or how many points you get for activities or questionnaires. Your profile will not be shared with others, neither with the other entities within a.s.r., nor with external parties. Your rights as mentioned in section 11 also apply to the user profile at Vitality.

11. What are your rights?

You have a number of rights related to your personal data. You can request to exercise these rights at privacy@asr.nl. We will respond to your request within one month. If we need more time to process your request, we will let you know within one month and tell you why we need more time. To process a request, we ask verification questions to identify you. We do this to prevent your data from ending up with someone else.

If someone else does make a request on your behalf, we would also like to receive an authorisation to confirm that that person is authorised to make this request on your behalf. You can read which rights this involves below:

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 changed. Also check your a.s.r. account, where you can see most of your data directly.

b. Having your data removed and the right to 'be forgotten'
In some cases and under certain conditions, you have the right to have the personal data we hold about you deleted. This may be the case if:
- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.
- you have withdrawn consent to processing.
- you raise legitimate objections to the processing.
- your personal data have been unlawfully processed by us.
- it concerns personal data of your child, 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 remove 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 are unable to comply with your request.

c. Restriction of the processing
If you believe we are processing your personal data unlawfully, you can request a restriction of the 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 you have provided to us for the performance of a contract you have concluded with us or based on your consent. This concerns only personal data we have received from you and not data received from third parties. The purpose of this right is to allow you to easily transfer these data to another party.

e. Right of 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 this case, we will no longer process your data, unless there are compelling legitimate grounds for the processing which outweigh your interest or relate to the instituting, exercising or substantiating of a legal claim.

f. Unsubscribing from personalised offers
You have the right to unsubscribe from newsletters or personalised offers through various channels (e.g. email, telephone and post) about our insurances and other (financial) services. In commercial offers we always point to the possibility to unsubscribe. Our staff may call you for commercial purposes. If we call you, you can indicate during the call that you do not want to be called again. You can also contact us yourself and let us know you don't want to be called anymore. When we create profiles (see above under 13) to make personalised 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.

12. Social media (e.g. chat, Whatsapp, Facebook)

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 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.

13. How we deal with profiling and automated decision-making

According to the GDPR, automated decision-making is the automated processing of personal data without "any human intervention". Profiling also involves automated decision-making where personal data are processed with the intention of assessing or predicting "personal aspects" such as a person's behaviour.

Profiling
We create profiles of our customers based on the data we have obtained from you and sometimes supplemented by information collected from public sources. We use such profiles to analyse data in order to manage risks, make connections and obtain insight into (future) actions and preferences, among other things. We create these profiles to improve and further tailor our services and the range of products and services we offer to you. For example, by using these data to estimate the premium or to send customers targeted advertisements/information. But also to combat fraud and prevent money laundering and terrorist financing.

When using profiling, we will first examine whether and what risks are involved, among other things to ensure that no incorrect picture of someone can be created. If we use profiling, you always have the right to object and in some cases we have to ask for consent.

Automated decision-making
We use automated processes, for example, to assess an insurance application, claim, a claim notification or when making a payment. For example, when you apply, the data you have entered are automatically assessed against our acceptance criteria. This way, we can make a risk assessment of your application. When you make a claim, the details you have entered are automatically checked against our claim assessment criteria. This way, we can assess whether a claim is covered. In both processes, we check whether the data are correct and the decision is made based on the data you entered, risk data, fraud data and data from (public) sources such as the CIS database, among other things.

If the outcome is that the application can be accepted or the claim paid out, then the application can be automatically accepted or the claim paid out automatically. You have the right to present a staff member with an automatically generated decision and ask for an explanation. You have the opportunity to let us know what you think and object to an automatically generated decision.

In principle, your data are processed automatically when you apply for basic or supplementary health insurance. This is done on the basis of the details you entered on the (electronic) application form. In addition, authorisation requests and claims go through a careful process, assessing whether your request or claim is covered by the insurance conditions. Assessing these criteria can be automated. You will always receive a message granting or rejecting the application or claim. You have the right to present a staff member with an automatically generated decision and ask for an explanation. You have the opportunity to let us know what you think and object to an automatically generated decision.

We may make use of Artificial Intelligence (AI) in this context. Before using AI, we assess whether its deployment is ethical, socially responsible and reliable. See further under 14.

14. How do we handle your personal data when we make use of Artificial Intelligence (AI)?

We use AI to (develop and improve) our processes and services. When developing or deploying AI, we may use personal data. Consider, for example:
- personal data used to train an AI system by analysing large amounts of personal data. These personal data are needed to validate certain outcomes of the AI system.
- personal data used by an AI system to make a decision. For example, when an AI system decides whether to accept the application for insurance.

When developing or training AI, controls are always built in to prevent undesirable outcomes for you as a customer but also for a.s.r., such as avoiding discrimination, bias and unfair treatment. In addition, the use of AI requires a study assessing the necessity and risks associated with such processing.

This means, among other things, that processing of personal data must comply with the requirements of the GDPR. When using personal data in AI, we work in compliance with the General Data Protection Regulation (GDPR), the GDPR Implementation Act (UAVG), the AI Regulation and the Dutch Code of Conduct for the Processing of Personal Data by Insurers (Gedragscode Verwerking Persoonsgegevens Verzekeraars). To this end, we conduct a data protection impact assessment (a DPIA) prior to the procurement, development and/or commissioning of an AI system where necessary. We opt for an AI system that processes as little potentially sensitive data or personal data as possible (data minimisation) and/or where there is the possibility to increase privacy through, for example, encryption, pseudonymisation/anonymisation or aggregation. We ensure the thorough protection of (training) data against corruption, contamination or hacking.

Within a.s.r. we can use AI systems for the following purposes:
- service/customer service optimisation, e.g. automatic analysis and classification of emails to handle them faster and better.
- for creating summaries of chats, whats-app or phone calls; this allows us to help our customers in a more targeted and proactive way,
- interpreting telephone customer queries and answering them more efficiently.

15. Amendment of the privacy statement

Privacy legislation is not static. We may therefore update this privacy statement to remain up to date. We may also amend our privacy statement if there are changes in the way we handle your data. We therefore recommend you to regularly check this privacy statement when visiting any of our websites. If there is a material change to this privacy statement, we will provide you with a clear notification (e.g. on our website).

16. Any questions or complaints?

Where to go if you have a question?
Do you have a question about this Privacy Statement? If so, please send an email to privacy.office@asr.nl.

You can contact the Data Protection Officer by sending an email to anl.compliance.fg@asr.nl.
Or a letter to:

a.s.r.
T.a.v. de Functionaris Gegevensbescherming
Postbus 2072
3500 HB Utrecht

Where to go if you have a complaint?
If you have a complaint about the use of your personal data,
you can report this to us via the complaint form on our website https://www.asr.nl/over-asr/klacht. Or contact us at https://www.asr.nl/contact.

If you have an Aegon product, you can use the complaint form on the Aegon website.

You can also file a complaint with the Dutch Data Protection Authority. In the Netherlands, this is the independent authority set up to monitor compliance with the General Data Protection Regulation. Website: https://www.autoriteitpersoonsgegevens.nl. Phone: +31 (0) 70 888 85 00

The privacy statement was last updated on 2 January 2025.

Download
- Privacy Statement ASR Nederland N.V.

For people who are or have been employed by ASR Nederland N.V., the Privacy Statement Employees is applicable.

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

ASR Nederland N.V., KVK 30070695 Utrecht

50436EN_1224