

Privacy statement ASR Nederland N.V.

1 Who we are

ASR Nederland N.V. has been designated as the party responsible for the processing of personal data by the following brands: a.s.r., De Amersfoortse, Ditzo, Ardanta and Europeesche Verzekeringen.

Visiting address:
Archimedeslaan 10
3584 BA Utrecht

Postal address:
PO Box 2072
3500 BA Utrecht

[Facebook](#)

[Twitter \(asr\)](#)

[WhatsApp: 0623889539](#)

[Telephone: \(030\) 257 9111](#)

2 What data do we process about you?

When you or your employer applies for insurance, a banking product or other financial service 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: adviser) or directly, for example via the website, email or telephone.

a. Name and address details

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

- When you visit our websites, we collect information about your visit through cookies and cookie settings.
- 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 email address). We use these data to implement the (insurance) agreement that we have concluded with you.
- If you're applying for a job with us, we will ask for your CV, any diplomas or the results of assessments and possibly other personal data. We will keep these data, after you've given us permission for this, up to a maximum of 12 months after your job application.

b. Financial data

If you are a customer with us, we will use your bank account number to make payments and collect payments and to transfer the claim amount we owe you.

We also have your salary data if you have one of our financial products, such as a pension account, an income insurance or a mortgage.

c. Additional data

For some insurance policies we will need additional information from you, such as your car registration in case of a car insurance, your profession or health data*. We will use these data, among other things, to make a proper assessment of the insurance risk, to set the conditions of the insurance and to assess any insurance claims.

*** Health data**

For acceptance or execution of mortgage, life, healthcare and income insurance policies and for personal injury settlement we need information about your health situation. Occasionally we may need information from your physician. If we need data from your physician, we will always ask your permission first.

Our staff will only process healthcare data they need to carry out their tasks. They have a duty of confidentiality in respect of the data they process. The processing of your healthcare data takes place within a specially separated unit (functional unit), under the responsibility of our medical adviser. This is a [BIG](#)-registered medical specialist. We comply with the rules of the [Beroepscode](#) voor Geneeskundig Adviseurs werkzaam in Particuliere Verzekeringzaken en/of Personenschadezaken (the professional code for medical advisers involved in private insurance cases and/or personal injury cases).

Are you involved in, for example, a bodily injury claim or an occupational disability claim? You will then receive a separate brochure for individual insurance policies containing an explanation of the use of your data.

For the basic insurance, we do not need any health information 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. For the supplementary insurance, we are free to decide whether or not to insure you on the basis of risk selection. You will be notified of this. However, we do process health data for the administration of both insurance policies.

For the risk assessment for non-life and income insurance, we ask you to provide information about any criminal record*.

***Criminal record**

You do not need to report any criminal offences that occurred more than 8 years ago. Criminal data on your application form, for example, will only be processed by us by employees who are authorised to do so.

d. Citizen service number (BSN)

In some cases we also process your citizen service number (BSN). For example, in case of pension insurance policies or mortgages. We only process your BSN if we have a statutory basis for this.

e. Data on your contacts with us

We process data about the contact you've had with us:

- What was the contact about (product, advice, an offer, a service call, message, complaint, information).
- When did this contact take place and with which department.
- How (via post, chat, our website, email, newsletter, app, adviser, web care team).

We use these data to see what our previous contact was about. Did it concern a question or a complaint or an advice on a complex product? Then we will be able to find it in the customer file and give you a proper response next time we have contact. We can record and save chat and telephone calls*

***Recording and saving calls**

We record telephone calls and save these for training and coaching purposes, to check transactions, to prevent and combat fraud and to be able to meet our statutory obligations. Recorded calls are not kept

any longer than necessary, the period varies depending on the brand and the purpose for which they were recorded. Calls recorded for training and coaching purposes are in general destroyed after 4 weeks. Calls to check transactions are kept for 7 years. We are statutorily required to do so. 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.

3 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 or other (external) parties such as Statistics Netherlands (CBS), the Credit Registration Office (BKR), the Employee Insurance Agency (UWV), working conditions services or market research firms. In our processing register we record from which sources we have received data if we know these sources. We inform you as much as possible about the sources from which we obtained the data.

4 Why do we process your data?

Purposes for the processing of personal data are:

a. For the performance of our services.

We use your contact details to contact you, to check whether you are a customer with us and to carry through any changes in your policies. **We may use your data to manage your products - or the products of your employer, such as absenteeism insurance policies - and for claims and damage settlement.**

b. Reduce risks

We also use your personal data to reduce risks, for example by:

- saving your IP address when you're visiting our website. We use your IP address to improve our services. In exceptional cases, we may investigate who's behind an IP address, for example to tackle fraud.
- to ensure adequate security. Consider for example user names, passwords and control questions.
- to conduct an internal quality inspection into the possible problems and risks and to assess whether legislation and regulations have been properly introduced.
- to ensure that we remain a healthy company (risk management).

c. Perform marketing activities

We will be 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're already using and which you are not. We do this by using cookies, for example. See our cookie policy for more information about this.
- collecting your choices and searches for example when you visit our web pages or apps and open emails such as the newsletter. These we analyse. For example, you may be interested in a car insurance when you visit a page on care insurance products.
- 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? No problem, if available you can arrange many things yourself via your personal environment.

d. Improve and innovate

We also use your personal data to make our products and services much more personal. We do this by combining and analysing them. These analyses bring us new ideas and better solutions. Based on these analyses, we may for example:

- Solve the cause of complaints, improve pages and forms on the website en 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 reports of our analyses and insights thus providing information services at aggregate level. Where possible, we remove the personal data that we do not need when drawing up analyses. And we may bundle data at a certain abstraction level (aggregate), encrypt (pseudonymise) or anonymise them.

e. Tracing fraud and abuse

When tracing fraud, abuse and improper use, we also record data. In doing so, we comply with the Insurers and Crime [Protocol](#) and the Financial Institutions Incident Warning System [Protocol](#). Both protocols have been drawn up by the Dutch Association of Insurers.

The PIFI includes the Association of Insurers, the Dutch Banking Association, the Mortgage Fraud Prevention Foundation, the Association of Finance Companies in the Netherlands and Health Insurance Companies in the Netherlands.

5 What is the legal ground for using your personal data?

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

- a. You have given permission*.
- b. The processing is necessary for the performance of the agreement, for example an insurance agreement or a mortgage loan agreement.
- c. The processing is necessary to meet a statutory obligation*, for example requesting a copy of an ID to identify you.
- d. The processing is necessary to promote a justified interest, for example when we conduct an investigation into possible fraud. 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.

***Permission**

We will only ask you for permission if that's necessary to process your personal data. When we process your personal data on the basis of your permission, you may withdraw your permission at any time. You can do this by contacting us, by telephone or email. In our newsletters, we state our contact details at the bottom.

***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're obliged to provide data to the Tax and Customs Authority (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, we cannot enter into an agreement with you. If we do not have data, or inaccurate data, about your criminal record, we cannot enter into an agreement with you, or if an agreement had already been concluded, we may terminate it if the information you provided is incorrect.

6 How do we secure your data?

We handle your data carefully and take the necessary technical and organisational measures* to safeguard an adequate protection level.

***Technical and organisational measures**

We have put in place technical and organisational measures to protect your data against loss or unlawful processing. For example, measures to use our website and IT systems safely and avoid abuse. But also protection of physical spaces where data are stored. We have an information security policy in place and arrange training programmes of our staff in the area of personal data protection. Only authorised staff can view and process your data.

All our employees have taken an oath or have made a solemn affirmation. Employees promise or state that they will comply with the legislation and regulations and codes of conduct and will act ethically.

7 How long do we store your data?

We do not store your data longer than necessary. In certain cases the law provides how long we may or must store data. In other cases we have determined how long we need to store 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. A quotation that has not resulted in an agreement in general will be removed after several months. A recorded telephone call often already after 4 weeks.

If you have specific questions about this, please contact the Data Protection Officer.

8 With whom do we share your data?

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

a. Within ASR Nederland N.V..

Are you a customer of one of the brands De Amersfoortse, Ditzo, De Europeesche Verzekeringen that come under ASR Nederland N.V.? (This does not apply for Ardanta.) In that case we may exchange your personal data - except for your health data - with one of the other brands of ASR Nederland. We do this, for example, to ensure a responsible acceptance policy and to prevent fraud.

In addition, we exchange information between the various departments of ASR Nederland, for the processing of your application or to obtain an overview of the products and services supplied to you. As a result, we can be of better service to you and you only need to pass on any change of address once, for example.

You may receive offers for other products of the brands that come under ASR Nederland N.V. This does not apply for Ardanta. If you do not want any offers for other products, you can indicate this.

If you have an adviser, you will only receive messages from us in consultation with your adviser.

b. The authorities

Sometimes we are statutorily required to pass on certain personal data to the authorities. For example the Tax and Customs Administration, the Employee Insurance Agency, the police, the judiciary, or regulators such as the Dutch Central Bank, the Netherlands Authority for the Financial Markets (AFM) and the Dutch Data Protection Authority.

c. Service providers and companies we work with

If statutorily permitted, we may exchange the data necessary for the service with your adviser. Sometimes we will need your permission for this.

We also engage other companies to perform services for us relating to the insurance agreement. For example debt-collection agencies, loss adjustment firms, the working conditions service, lawyers or a reinsurer. With these parties, we lay down agreements to safeguard your privacy.

We may also outsource the processing of personal data to third parties, the so-called processors. For example, we make use of IT service providers for maintenance and support functions. These IT service providers are to be considered as processors because they do not have independent control of the personal data that are made available by a.s.r. to the IT service provider in the context of the service. In these situations, ASR Nederland N.V. remains responsible for the careful processing of your data.

d. CIS databank

To ensure a sound acceptance and risk policy and to prevent fraud, we record your data in the Central Information System of the Foundation CIS in The Hague. Foundation CIS is a foundation that can support insurers in acceptance and claims processes. With the information affiliated with the CIS we may, under strict conditions, exchange information via the Foundation CIS. More information on this can be found on the website of [Foundation CIS](#).

e. External Reference Register (EVR)

Financial institutions can record behavior of (legal) persons who have led or could lead to the detriment of financial institutions in an Incident Register. An External Reference Register is linked to this Incident Register. This External Reference Register contains only referral data (for example a name and date of birth or Chamber of Commerce number) that may be included under strict conditions. Every financial institution that is affiliated with one of the participating trade associations has access to (a part of) the External Reference Register.

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

If we share data with a service provider outside the EEA, we make arrangements with them so that we will at all times abide by the rules agreed in the European Economic Area. In doing so, we make use of the Standard Clauses; this is a model endorsed by the European Union in which it is agreed that a sufficient protection level for the protection of personal data is put in place.

9 What are your rights?

a. Viewing or correcting data

You have the right to ask us what personal data we process about you and to have incorrect data adjusted or deleted.

First, you can view or correct your data in your personal environment (if available) or you can contact us via the usual channels (mail or e-mail).

We will ask verification questions or ask you for a copy of your proof of identity* to identify yourself.

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 us with 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 removed. 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 permission to process them;
- you file a well-founded objection against processing;
- your personal data have been unlawfully processed by us;
- pursuant to a statutory obligation to remove 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 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 removed, 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, or that the data processed by us are incorrect, you may request that the processing be restricted. This means that the data may no longer 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.

f. Unsubscribing from personal offers

You have the right to unsubscribe from newsletters or personal offers for our insurance and banking products and other financial services. In commercial offers we always point to the possibility to unsubscribe. Our staff may call you for commercial purposes. In doing so, we will adhere to the rules of the Do-not-call-me register (Bel-me-niet register). On the website www.bel-me-niet.nl you can unsubscribe your telephone number for commercial calls. Bel me niet register doesn't apply when you are a customer of the organization of company.

10. Email and social media (chat, Whatsapp, Facebook)

1. Email

Before we communicate with you via email, we will ask your permission for this, unless you have already given us permission. You can withdraw your permission at any time.

2. Social Media

You can opt to chat with us, 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 store 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 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.

11. Adjustment of the privacy statement

The privacy legislation is not static. Therefore we can adjust this privacy statement in order to keep 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 on visiting one of our websites. We can also inform you retroactively about changes in this privacy statement through a pop-up banner, mail, a news report on our websites or via your personal environment (if available).

12 Profiling

We make profiles of our customers on the basis of the data we collect with the purpose of analysing these data and thus obtaining insight into (future) actions and preferences. We can then anticipate these. For example sending targeted advertising/information to customers based on their surfing behaviour that has been followed via tracking cookies. 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.

13. Any questions or complaints?

Do you have questions about this privacy statement? Please contact the Data Protection Officer of ASR Nederland N.V. Send an email to: privacy@asr.nl or send a letter to:

a.s.r.
Attn. the Privacy Officer
Afdeling Integriteit (Integrity department)
PO Box 2072
3500 HB Utrecht

If you have any complaints about privacy, please contact us via our complaint form on our website. You can also file a complaint with the Personal Data Authority (www.autoriteitpersoonsgegevens.nl tel. 0900-2001201).

Privacy statement most recently updated 13 September 2018