



Employee

Privacy Statement

Contents

Who are we?	3
How do we handle your personal data?	3
What personal data do we process?	3
How do we obtain your data?	4
Why do we process your data?	4
On what basis do we process your data?	5
Consequences of not processing personal data	5
How do we protect your data?	6
How long do we keep your data?	6
With whom do we share your data?	6
Transfer of personal data outside the EEA	7
Any questions or complaints?	8
Adaptation of the privacy statement	8

Employee Privacy Statement

This privacy statement applies to employees working at ASR Nederland N.V. (hereinafter 'a.s.r.'). By employees we mean persons who work (or have worked) on the basis of an employment agreement with a.s.r. or persons who perform (or have performed) work for a.s.r. other than on the basis of an employment agreement (hereinafter 'employee') and, where relevant, their relatives including family members. This privacy statement explains how we handle your personal data and applies from the moment the hiring process has started (directly or through a third party) until the moment you are no longer employed by us (or longer to the extent we still (need to) process personal data).

This privacy statement does not apply to candidates interested in working at a.s.r. or to job applicants. These employees are subject to the Candidate Privacy Statement www.werkenbijasr.nl/privacyverklaring.

Who are we?

ASR Nederland N.V. is the controller and point of contact for the processing of personal data by the following entities and brands (which may be (co-)responsible for the processing of personal data): 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 Premiepensioeninstelling N.V., ASR Vooruit B.V., ASR Re-integratie B.V., Ardanta and Loyalis.

Visiting address:
Archimedeslaan 10
3584 BA Utrecht

Postal address:
Postbus 2072
3500 HB Utrecht

How do we handle your personal data?

a.s.r. and all its brands handle your personal data with due care. In doing so, we adhere to applicable (privacy) legislation. All employees must observe confidentiality and they have taken an oath or have made a solemn affirmation to act with integrity and due care.

What personal data do we process?

If you are or have been employed by a.s.r., we have your (personal) data. The data we may process include:

- basic personal data (such as name, address, date of birth, gender, telephone number and email address);
- job-related information (such as employee number, start/end of employment, contract duration, part-time percentage, office location, department, job title);
- financial data (such as salary, pension, IBAN (account) number, allowances, attachment of earnings, taxes and contributions paid by a.s.r.);
- performance-related information (such as evaluations, job appraisals);
- development-related information (such as training programmes, courses, assessments);
- IT/work location/workplace-related data (such as license plate registration, access card number, workplace check, devices and tools you receive (on loan) from a.s.r., token, IP address, email address, access rights and their use).

Special or sensitive personal data

We also process some special or sensitive personal data, such as citizen service number (BSN). Sometimes we process information about your health, such as data on absenteeism, reintegration, maternity leave. For example, we may also request information about your criminal record. We process these data only when necessary to comply with legislation and regulations. Special or sensitive personal data are processed only by employees authorised to do so.

How do we obtain your data?

In most cases, we obtain the data directly from you. Third parties may also provide us with your personal data which we then process. For example a recruitment partner, such as a recruitment agency or an temporary employment agency. From employees with partially-reduced work capacity, we also receive data from the Employee Insurance Agency (UWV), local authorities and job coaching organisations, for example.

Why do we process your data?

We process your personal data only for the following or compatible purposes:

- To perform the (employment) agreement in the broadest sense. This applies both at the start of, during and at or after the termination of the employment relationship. These include drafting an (employment) agreement, implementing employment conditions, applying in-house medical care, training and determining severance pay.
- To keep accurate and complete records of your personal data.
- To determine the amount of net (travel) expense allowance.
- To comply with legal requirements.
- To provide access to the buildings and parking facilities.
- To manage the quality of our services.
- To manage, make (work) processes more sustainable and efficient.
- To facilitate and support employees, including in the field of ICT.
- To secure data, employees, visitors, buildings and equipment.
- To prepare and execute business transactions such as mergers or acquisitions.
- To prevent and be able to stop fraud or theft or other unethical behaviour.

For these or compatible purposes, a.s.r. may process your personal data. This includes collecting, recording, organising, storing, using, disclosing, assembling and otherwise processing personal data. Also, a.s.r. may process your personal data into an anonymised or non-anonymised (aggregated) file, for example for (market) research or data analysis.

a.s.r. may also process your personal data in the following cases:

Pre- and in-employment screening

Everyone who starts working at or for a.s.r. is screened beforehand. We do this to assess the integrity of our employees. The screening process will at least involve checking against the lists of the various incident registers of financial institutions and sanctions lists. An inventory of your sideline activities also takes place. For positions identified as integrity-sensitive, additional screening is carried out by the security affairs department.

Your integrity will also be tested during the performance of your duties at a.s.r. This takes place once every three years.

Customer interactions

The recording of telephone (Teams) calls and the recording of screen actions, email messages, chats and social media (hereinafter referred to as (recording) customer interactions) is allowed only under strict conditions and for predefined purposes.

HR analyses

We also use your personal data to implement responsible, effective and efficient HR policies (people analytics). These statistical analyses focus on examining the impact of the HR strategy pursued. In principle, the results of the surveys and associated opinions are not directly traceable to individuals.

Monitoring

We monitor email, telephone and internet use to identify unauthorised and improper use and to ensure the security of the a.s.r. environment. In this context no distinction is made between business and private data in the digital a.s.r. working environment. a.s.r. ensures that your privacy is sufficiently taken into account. Monitoring by or at the request of a.s.r. takes place, in principle, at the level of aggregate data that cannot be traced back to individual persons. If you are suspected of breaching the rules, targeted monitoring may take place for a fixed (short) period.

Fraud, theft or other unethical behaviour

In the event of a concrete suspicion of fraud, theft or other unethical behaviour, we are authorised to process data traceable to you without prior notice. This includes data such as email, telephone and internet use, (customer) interactions and camera footage. In such cases, we may also, without prior notice, collect and record (historical) data through the use of (personnel tracking) systems and otherwise process data so that fraud, theft or other unethical behaviour can be terminated and disciplinary measures can be imposed on the employee(s) concerned.

Camera data

We use camera surveillance. Its purpose is to protect our company property and the property of our employees and visitors, secure access to the company premises and parking facilities, and record incidents. Camera surveillance takes place at the entrance to and inside our company premises, among other places. The cameras are visibly and invisibly suspended and their presence is made known through the use of signs.

Profiling and automated decision-making

At times, profiling may occur, for example when we ask you to take an assessment. Based on personal preferences you specify during an assessment, a profile of you will be created. We do not use automated decision-making.

On what basis do we process your data?

We only process your personal data for the above purposes if this is necessary

- for the conclusion and performance of an (employment) agreement.
- to comply with a statutory obligation or
- when this is necessary for a legitimate interest of a.s.r. or a third party.

a.s.r. may also request your consent in special cases. In that case, we will inform you exactly what you are consenting to. You can withdraw a given consent at any time. The withdrawal of consent does not affect the lawfulness of the processing prior to its withdrawal.

Consequences of not processing personal data

The personal data we request from you are necessary for the purposes mentioned above. If you do not provide these data, this may affect the hiring process and further performance of the (employment) agreement.

How do we protect your data?

We handle your personal data carefully and take the necessary technical and organisational measures to ensure an adequate level of protection. We have taken these measures to protect your personal data against loss or unlawful processing. We take great care to ensure optimal security of our systems in which personal data are stored. For example, measures to keep our website 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 hours a day. We have an information security policy in place and provide training for our employees on personal data protection. Only authorised employees who need access to your data can view and process your data. All our employees have taken the oath or made a promise to that end. Employees hereby promise or declare that they will comply with legislation and regulations and codes of conduct and will act with integrity.

How long do we keep your data?

We keep your personal data no longer than necessary for the purpose for which we collected your personal data or to comply with legislation and regulations. 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 drawn up a retention period policy for this purpose.

Most personal data of (former) employees are deleted no later than five years after the end of employment, unless they are still needed at that time to comply with a legal obligation incumbent on us. For example, due to applicable tax legislation, data relating to salary are kept for longer, i.e. at least seven years.

With whom do we share your data?

We only provide personal data to third parties if this is necessary for the aforementioned purposes and only on the bases stated in this privacy statement. Among others, we provide your personal data to the following third parties.

Within a.s.r.

We exchange your personal data within a.s.r. By this we mean brands and entities that fall under ASR Nederland N.V. We only make these data available to those within a.s.r. who need it because of their job. For example, in connection with implementing the pension scheme, the share plan or in case of monitoring etc.

Outside a.s.r.

We may also exchange your personal data outside a.s.r. In that case, we exchange your personal data with business relations such as the occupational health and safety service, trainers, service providers, Stichting Kunst & Historisch Bezit ASR Nederland and (if necessary to comply with legislation and regulations) authorised government bodies (e.g. UWW, the Tax and Customs Administration). We do not share all your data, but only that which is necessary for the third party.

We may also outsource the processing of your personal data to third parties, for example an IT supplier. Where we remain responsible for processing your personal data, we make clear agreements with these parties to safeguard your privacy.

Your personal data will not be resold.

Transfer of personal data outside the 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 the Standard Contractual Clauses, for example (European model contract provisions). We make clear agreements with parties so that processing takes place in accordance with European legislation.

What are your rights?

You have the right to access, correct or delete your personal data. In addition, you have the right to withdraw your consent to data processing or object to the processing of your personal data. Where necessary, before we can respond to your request, we may ask verification questions or request additional information to identify you. You can exercise your rights by sending a request to hr@asr.nl.

If we do not or cannot comply with your request, we will give you the reasons why we are unwilling or unable to do so.

a. Accessing or correcting data (inspection and rectification)

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

To view your digital personnel file maintained by the HR department, you need to make an appointment with HR.

You can request a copy of any documents in your personnel file. We will not provide a copy if it violates another person's right to privacy.

b. Request for data to be deleted

In some cases and under certain conditions, you have the right to have the personal data we hold about you deleted. This is the case if:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- you have withdrawn your consent to processing;
- you raise legitimate objections to the processing;
- your personal data have been unlawfully processed by us;
- there is a statutory obligation to delete the personal data.

c. Right of objection

You have the right to object at any time to the processing of your personal data carried out on the basis of a legitimate interest of a.s.r. or a third party. In this case, we will no longer process your data, unless there are compelling legitimate grounds for the processing which outweigh or relate to the instituting, exercising or substantiating of a legal claim.

d. Right to restriction of processing

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

e. Right to transfer 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 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.

Any questions or complaints?

Do you have questions about the Employee Privacy Statement, or do you need more explanation on how we handle your personal data and your privacy as an employee? Please contact HR by sending an email to hr@asr.nl. You can also contact them in case of complaints regarding the processing of your personal data.

You can also contact the Data Protection Officer of ASR Nederland N.V. Please send an email to privacy@asr.nl or send a letter to a.s.r., for the attention of the Data Protection Officer. Our address is:

a.s.r.
Attn. the Data Protection Officer
Afdeling Integriteit (Integrity department)
Postbus 2072
3500 HB Utrecht

You can also file a complaint at any time with the Personal Data Authority (www.autoriteitpersoonsgegevens.nl, tel. 088-1805250).

Adaptation of the privacy statement

Privacy legislation continues to evolve. We may update this privacy statement to keep it up to date. We do so in the event of new developments, for example if something changes in our business activities or in legislation or the case law. We therefore ask you to consult this privacy statement regularly to keep yourself informed. If there is a material change to this Employee Privacy Statement, we will provide you with a clear notification (e.g. on our website).

This Employee Privacy Statement was published on 1 May 2023.

