Privacy policy

We respect your privacy. Our organization is committed to preserve your privacy as much as possible. Confidentiality is observed with regard to any information you provide to us. When processing personal data, we observe the applicable laws and regulations in privacy. This privacy policy informs you about the way in which we handle your data.

Scope of application

This privacy policy applies to AHG Holding B.V. and its operating companies:

- Active Health Group B.V.
- Active IT Lab B.V.
- Atrium Adviesgroep B.V.

Categories of personal data

When you make use of our services certain (personal) data may be collected as follows:

- Organizational advice / DZI Consultancy / HCBI
  - Name / Address / City
  - Contact details

- Preventive medical check (PMO 2.0) / PAGO (Periodical Occupational Health check) / medical checks:
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Health data

- Employability / resilience / lifestyle coaching
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Health data

- Reintegration coaching
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Curriculum Vitae
  - Health data
  - Citizen service number (BSN) (only UWV clients)

- Career coaching / outplacement
  - Name / Address / City
  - Contact details
  - Date of birth

  - Gender
  - Curriculum Vitae

- Other employability expertises
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Health data

- Education
  - Name / Address / City
  - Name of organisation
  - Contact details
  - Date of birth
  - Gender
  - BIG number

- Occupational health expert services
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Curriculum Vitae
  - Salary details

- Absenteeism supervision
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Citizen service number (BSN)
  - Health data
  - SFB status (structurally functionally limitations status)

- Second opinion / Objection & Appeal
  - Name / Address / City
  - Contact details
  - Date of birth
  - Gender
  - Citizen service number (BSN)
  - Health details

- Complaint handling
  - Name / Address / City
  - Contact details
  - Health data

- Financial administration
  - Name / Address / City
  - Contact details

  - Financial data

- Marketing & Communication:
  - Contact details

- Sales
  - Name / Address / City
  - Name of organization
  - Contact details

- Job application
  - Name / Address / City
  - Contact details
  - Gender
  - Date of birth
  - Curriculum Vitae
  - BIG number
  - Passport photo

- Visiting a site:
  - Name
  - Date of visit
  - Arrival time
  - Departure time

Basis for data processing

We may only process personal data on a so-called legal basis. Our services usually involve the performance of legal obligations and/or the provision of healthcare. These principles can be found in Articles 6 paragraph 1 sub c and 9 paragraph 2 sub h of the General Data Processing Regulations (GDPR).

We could also have an agreement with you for our services; in that case, the performance of this agreement is the legal basis according to article 6 paragraph 1 sub b GDPR.

If we wish to process your data for marketing & communication purposes, we ask for your consent; we will do so in accordance with Article 6 paragraph 1 sub a GDPR. A justified interest in marketing & communication purposes provides another basis; in that case article 6 clause 1 subsection f GTC applies. For anonymised information processing using Google Analytics as specified in these privacy regulations for 'Cookies', article 6 paragraph 1 under f of the GDPR applies.

In the event of processing your data for sales purposes, the legal basis is article 6 clause 1 subsection f GDPR.

For the processing of your application data, we first ask you for permission; you will find this basis in article 6 paragraph 1 sub a GDPR.

Without your data we are unable to execute our services or inform you about our services. Unfortunately, if you would like us to destroy your data, this usually means we'll have to stop our services and communication with you.

Sources

We receive your personal data from you, your employer and third parties with whom we cooperate such as the UWV (Employees Insurance Agency).

Purposes of data processing

Personal data collected by us will be used for the following purposes:

- Performance of our services such as organizational advice, preventive medical examinations, medical checks, coaching, and courses including possible complaint management.
- Providing information about our activities, and
- Carrying out the application procedure, and
- Accounting and financial settlement.

Access to personal data

Within our organization, we apply the following principles regarding access to personal data:

- Employees of our organization only have access to personal data to the extent necessary for the proper performance of their duties and are contractually bound to secrecy.
- Authorizations for information systems shall be granted only to officials in job groups to whom access is necessary pursuant to the performance of their duties. An authorization matrix specifies the authorizations up to the level of the type of rights: none, reading, editing.
- External parties hired by us or otherwise appointed to perform work have access to personal data to the extent necessary for the proper performance of their duties and are contractually bound to secrecy.
- Electronic (medical) personal data are secured in such a way that unauthorized persons cannot gain access to these data.
- For each category of data, it is indicated below from which job function(s), which access is provided to which data.

Organizational advice / DZI Consultancy / HCBI	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Occupational health doctors	T	-
Occupational health doctors in training (AIOS) / basic practitioners (ANIOS)	T	-
Core experts: higher safety expert, occupational hygienist, occupational & organization expert	T	-
Consultant	T	-
System administrator	T	-
Employee Quality / Quality Manager	T	-
Employee Security / Manager Security	T	-
Management	T	-
Board	T	-

Preventive medical check (PMO 2.0) / PAGO / medical checks	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee PMO (2.0)/ PAGO / medical checks	T	Conditionality of task delegation Occupational health doctor
Project Manager PMO (2.0) / PAGO / Medical checks	T	Conditionality of task delegation Occupational health doctor
Occupational health / medical doctors	T	T

Occupational health doctors in training (AIOS) / basic practitioners (ANIOS)	T	Conditionality of task delegation Occupational health doctor
Lifestyle / Vitality coach	T	Conditionality of task delegation Occupational health doctor
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager PMO (2.0) / PAGO / medical checks	T	-
Board	-	-

Employability / resilience / lifestyle coaching	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Backoffice AHC	T	T
Coaches	T	T
System administrator / Functional application administrator	T	T
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	T
Manager Backoffice AHC	T	T
Board	-	-

Reintegration coaching	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Backoffice AHC	T	T
Coaches	T	T
System administrator / Functional application administrator	T	T
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	T
Manager Backoffice AHC	T	T
Board	-	-

Career coaching / outplacement	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Backoffice AHC	T	-
Coaches	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Backoffice AHC	T	-
Board	-	-

Education	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Backoffice AHC	T	-
Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Backoffice AHC	T	-
Directie	-	-

Occupational health expert services	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Backoffice AHC	T	-
Occupational health expert	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-

Employee Security / Manager Security	T	-
Manager Backoffice AHC	T	-
Board	-	-

Absenteeism supervision	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
(administrative)-Case Manager	T	Voorwaardelijkheid taakdelegatie Bedrijfsarts
Occupational health doctors in training (AIOS) / basic practitioners (ANIOS)	T	Voorwaardelijkheid supervisie Bedrijfsarts
Occupational health doctor	T	T
Support	T	T
Occupational health expert	T	T
Core experts: higher safety expert, occupational hygienist, occupational & organization expert	T	-
System administrator / Functional application administrator	T	T
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	T
Manager operational	T	T
Board	-	-

Second opinion / Objection & Appeal	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
(administrative)-Case Manager	T	Voorwaardelijkheid taakdelegatie bedrijfsarts
Occupational health doctors in training (AIOS) / basic practitioners (ANIOS)	T	Voorwaardelijkheid supervisie bedrijfsarts
Occupational health doctor	T	T
Occupational health expert	T	T
Employee Backoffice AHC	T	-
System administrator / Functional application administrator	T	T
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	T
Manager operational	T	T
Manager Backoffice AHC	T	-
Board	-	-

Complaint handling	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Complaints handler	T	T
System administrator / Functional application administrator	T	T
Employee Quality / Quality Manager	T	-
Employee Security / Manager Security	T	-
Board	T	-

Financial administration	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Finance	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Finance	T	-
Board	T	-

Marketing & Communication	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**

Employee Marketing & Communication	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Marketing & Communication	T	-
Board	-	-

Sales	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee Sales	T	-
Account manager	T	-
Consultant	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Sales	T	-
Board	T	-

Application	**Standard personal data (name and address, passport photo and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Employee recruitment	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	-	-
Employee Security / Manager Security	T	-
Manager Recruitment	T	-
Board	T	-

Visiting a site	**Standard personal data (name and contact details)**	**Supplementary privacy sensitive personal data (health data)**
Hostess	T	-
Systeembeheerder / Functioneel applicatiebeheerder	T	-
System administrator / Functional application administrator	T	-
Employee Quality / Quality Manager	T	-
Employee Security / Manager Security	T	-
Management	T	-
Board	T	-

Provision of your personal data to third parties

Personal data shall only be provided to a third party when required by a statutory requirement or with the consent of the registered person or his authorised representative, or if the data processing is necessary to protect the legitimate interests of the third party to whom the data is provided.

A client's medical information is only provided to the employer or third parties with the client's specific written consent. This consent shall be included in the medical file.

No notice shall be given to the employer of an employee's visit to a working-conditions consultation or voluntary participation by an employee in periodic examinations. If, as a result of such a visit or participation, the company doctor wishes to give advice to the employer, the express and specific consent of the employee is required. This consent must be confirmed through a written authorisation. Such written consent shall be recorded in the medical file.

Retention periods

We will not retain your data for longer than is necessary for the purposes described above, unless required by law, which provision will be observed by us.

Medical dossier

The Civil Code 7, Section 5 The Agreement for Medical Treatment (WGBO) prescribes a statutory retention period for medical dossiers of 20 years or so much longer as ensues from the care of a proper and professional healthcare provider. In a situation where there is no treatment agreement, the medical dossier may be retained for as long as is necessary for the purpose of the study.

A medical dossier may contain:

- data collected in the context of social-medical assistance during absenteeism and reintegration;
- data from statutory and voluntary PAGO's, PMO's (2.0), preemployment medical checks, other medical checks and health checks;
- data collected during the working conditions consultation.

Social medical assistance

Medical dossiers created for social medical assistance are kept for up to 20 years from the time of the last addition or change. There are occupational diseases that can manifest themselves after a (longer) period of time. When this risk is present, medical data must be kept longer for this purpose.

PAGO's, PMO's (2.0), pre-employment checks, other medical checks and health checks

In voluntary situations, the WGBO applies in full.

In case of a pre-employment check, the Medical Check Act applies. If the employment contract is not concluded, the data collected will be destroyed as soon as possible. If the employment contract is concluded, the data shall only be included in the medical file with the consent of the employee. If the employee does not give permission, the data may only be kept separate for a limited period of time (no longer than 6 months).

Working conditions consultation

The WGBO applies in full.

Specific regulations

The Working Conditions Decree stipulates that the results of an occupational health check for employees who have been exposed to certain hazardous substances must be kept for at least 40 years after the end of their exposure.

The Radiation Protection Basic Safety Standards Decree stipulates that records of employees exposed to ionizing radiation must be retained until the employee has reached, or is believed to have reached, the age of 75, but for at least 30 years after the person has ended the activities.

Reintegration dossier

As the medical part of a reintegration file is in the possession of a care provider falling under the scope of the WGBO, a retention period of 20 years applies. There is no statutory retention period for the administrative, nonmedical part of a reintegration dossier. In principle, we keep this part no longer than 2 years after completion of the reintegration.

Administrative, nonmedical dossiers remaining

Medical checks/PMO (2.0)

There is no legal retention period for administrative, nonmedical data in examination/PMO (2.0) dossiers. In principle, we do not retain this data longer than 2 years after the examination has been completed. Exceptions to this are professional medical checks which are linked to a declaration of suitability to perform work; we do not save these in principle longer than 5 years after completion of the check.

Coaching dossiers, not being reintegration

There is no legal retention period for these dossiers. In principle, we keep these no longer than 2 years after completion of the process.

Education

There is no legal retention period for administrative data and proof of participation (non-recognised diploma) of education. In principle, we do not keep these for longer than 2 years after completion of the course.

Complaints

For the storage of complaints, we apply a period of 10 years in line with the period of the complaint law of the Disciplinary Board for Health Care.

Job application data

The standard retention period for job application data is 4 weeks after the end of the application procedure. If you give your permission for the data to be kept for a longer period, they will be kept for a maximum of 1 year after the end of the application procedure.

Other

Otherwise, if we have a contract with you, we will keep your data for as long as required by law; normally 7 years. If we do not have an agreement with you, we will keep your contact details for as long as we have a legitimate interest in doing so and you have not objected.

Cookies

On our websites www.activehealthgroup.nl, , www.activehealth.nl, and www.activehealthassurance.nl general visiting data are tracked via Google Analytics. We may use these data anonymously for statistical analysis and optimisation of the functioning of the website. This includes the following categories of data: IP address without last octet; time, country, place, language of query; browser used, operating system, service provider, screen resolution; number of visitors, sessions, bounce rates; page views, values, bounce rate, exit rate; average session duration; channel of visit. We have disabled Google's "data sharing with Google" features and do not use other Google services in conjunction with Google Analytics cookies.

Google's privacy policy is available at: http://www.google.com/privacypolicy.html.

You can set your browser to notify you when you receive a cookie or to allow or deny cookies in general.

Your rights

When we process personal data about you, you have various rights which you can exercise. For example, you have the right to access, rectify and delete your data. You can also request us to transfer data to you or another party or to limit the data processing. You are also free to object to the processing of your data. You can submit your request to us in writing by e-mail via melding@activehealthgroup.nl or by post. You will find our contact details on the last page of these privacy regulations. We aim to respond to your request within 14 working days.

Filing a complaint

In the unlikely event you might not be satisfied with our way of handling your personal data, your complaint can be submitted. With respect to this, we refer you to our complaints regulations on our website. You also have the option of submitting a complaint to the Personal Data Authority. Contact details of the Authority Personal Data can be found here: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens.

Amendments to this privacy policy

We reserve the right to amend this privacy policy. All changes will be announced on our website. We therefore advise you to consult our website regularly so that you are aware of any changes.

The original privacy document is written in Dutch and has been translated into English. While it is intended that both versions are identical, the possibility of any discrepancies between the Dutch version and English version might appear. In any case the Dutch version of the privacy policy will dominate.

Automated decision-making

We do not use your personal data to make automatic decisions about your treatment in any way. Consequently, no automated decision-making as referred to in article 22 of the GDPR takes place.

Our contact details

The formal controller is:
Active Health Group B.V.
Folkert Elsingastraat 38
3067 NW Rotterdam

For all your questions and comments about privacy and the protection of your personal data in our organization, please contact our Data Protection Officer:

Data Protection Officer
Active Health Group B.V.
Folkert Elsingastraat 38
3067 NW Rotterdam
T: +31-88-2866055
E: melding@activehealthgroup.nl

Document version: January 2022