Privacy policy for Avonova's customers

Version 1. 1

24 -08 - 27

Headquarters

Avonova Gruop

Phone: +385 (0)55 66500-6821

Klarastrandsviaduct 90 11164 Stockholm

Data Protection Officer

gdpr@avonova.com

avonova

Content

Glossary of concepts

In addition to the terms defined in running text, these definitions, whether used in the plural or singular, in definite or indefinite form, shall have the following meanings when specified.

Processing	An operation or combination of operations on personal data or sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, production, reading, use, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Data protection legislation	Means all privacy and personal data legislation, as well as other legislation (including regulations), applicable to the processing of Personal Data that takes place under this Privacy Policy, including European Union legislation and legislation of EU member states.
Controller	Natural or legal person, public authority, institution or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Instruction	The written instructions specifying the subject, duration, nature and purpose, type of personal data and categories of data subjects and special needs covered by the processing;
Contact person	Employed by a company, authority or organisation that is a customer of Avonova and who is Avonova's contact person or otherwise has contact with us in matters concerning Avonova's and the customer company's relationships.
Processor	Any natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;
Personal data	Any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, social security number, location data or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Breach of personal data	An event resulting in accidental or unlawful destruction, loss or alteration or unauthorized disclosure of, or access to, the personal data transmitted, stored or otherwise processed.
Data subject	Natural person if personal data is processed.

Third country	A state that is not part of the European Union or is not a member of the European Economic Area (EEA).
Sub-processor	Any natural or legal person, public authority, agency or other body, as a subcontractor to the data processor, processes personal data on behalf of the data controller.
Identity data	Data that enable you to be identified, such as your name
Contact details	Data that enable you to be contacted, such as address, e-mail address and phone number.
Profile data	Data related to your profile, such as the title, name and address of the company or organization you belong to.
Order data	Data about an ordered product or service, such as the product or service, price and delivery period or assignment period
Invoicing data	Invoicing data, such as payment conditions, cost centre or reference number.
Communication	Content contained in communications you have with us, such as the content of e-mails or responses that you submit when you fill in a questionnaire.

1. Introduction to Avonova

1.1 Avonova

Avonova offers services within occupational health and leadership development. With broad knowledge and commitment, we help organizations and their employees become more sustainable, communicate more effectively and feel better.

1.2 The aim of this policy

Avonova cares about your privacy, therefore Avonova has established this policy. It is based on applicable national and common European data protection laws. It clarifies how Avonova works to protect your rights and privacy. The processing of personal data is regulated by the EU General Data Protection Regulation ("GDPR").

The purpose of this policy is to let you know how Avonova works in terms of quality and how we process your personal data, what we use it for, who can access it and under what conditions and how you can exercise your rights when you are a contact person and have contact with us.

2. Avonova's responsibilities and obligations

2.1 Avonova's principles for personal data

Personal data shall be formulated and processed in such a way that respects the integrity of patients and other data subjects. Documented personal data shall be handled and stored in such a way that prevents unauthorised access.

Within a healthcare provider's activities, the staff who participate in the healthcare, or need the data for other reasons in their healthcare work, are the persons who are authorised to access data

2.2 Data Processor

Avonova Solutions OY is the data processor for its customers who use the system Avonova HR and HSE.

3. Processing of personal data

3.1 Where do we collect personal data

We collect personal data from:

- Your employer (name, address, e-mail address and organisational affiliation/group/department)
- Yourself (e.g. when you communicate with us via email)
- From other companies in the Avonova Group (e.g. name and e-mail address)
- From public registers (e.g. if you have the right to sign, the CEO or the chairman of the board of a company that is a customer of Avonova)

3.2 Why do we process your personal data?

Introduction

Below is more detailed information about why we use your personal data in different cases. To read more about which categories of data, based on which legal basis we use personal data for each purpose and how long your personal data is stored, please see our detailed information on the processing of personal data further down in this document.

Manage relationships with customers, vendors, and partners

When you are a contact person, we use your personal data to manage the customer relationship, for example to register you as a contact person, administer invoices and communicate for the same purpose.

Process orders

In order to process orders for customer services, we use your personal data where applicable when you are a contact person for this purpose, for example to handle order confirmations and communicate with you regarding your order.

Follow up and manage the customer relationship

We use your personal data as an individual when necessary to follow up and manage the customer relationship.

Answer questions and provide customer service

If you contact us, for example by e-mail or phone, we will use your personal data that you share with us, to answer your question; and to provide customer service.

Communication between our employees and external persons in the service

In connection with communication, for example via email, between our employees and external persons, we process your personal data where applicable.

Newsletter

We use your personal data to deliver our newsletters. You can unsubscribe from mailings at any time by clicking on the unsubscribe link in the email or by contacting us.

Follow up and evaluate the activities

We use your personal data to compile reports at an overall level, and statistics to follow up and evaluate our business.

Develop and improve activities

We use your personal information when conducting analyses to develop and improve our business, business practices and strategies.

Document our activities

We use your data to document our business, where applicable, for example to administer and store agreements, decision support and presentations.

Conduct events and other activities

If you participate in an event or other activity that we organize, we use your personal data to carry out the event or activity, for example to register your participation, to communicate with you about the event or activity, and to follow up on the event or activity.

Conducting surveys

If you choose to participate in a survey we conduct, we will collect the personal data you provide in connection with the survey. Your opinions about our business and services are important to us. You can unsubscribe from email at any time by clicking on the unsubscribe link in the email or by contacting us.

Ensure technical functionality and security

We use your personal data to ensure the necessary technical functionality and security for our IT systems, for example within security logging, error handling and backup.

Process and respond to legal claims

We process your personal data if it is necessary to handle and respond to a legal claim, for example in connection with a dispute or legal process. For this purpose, we may share certain information with other recipients who have a legal right to do so, see below for more information.

Comply with legal obligations

In order to comply with legal obligations that we have, we process your personal data if necessary, for example to comply with the requirements of health legislation and of accounting or data protection legislation. For this purpose, we may share certain information with other recipients who have a legal right to do so, see below for more information.

3.3 Rights

3.3.1. Right of access

The data subject has the right to contact Avonova, which is the data controller, and request access to the personal data that Avonova processes and information about, among other things, the purpose of the processing and with whom the personal data has been shared.

Avonova shall, at the request of the data subject, provide a copy of the personal data processed free of charge. In case of additional copies, Avonova may charge an administration fee.

3.3.2 Right to rectification, erasure or restriction

The data subject has the right to have his/her personal data rectified without undue delay or, under certain conditions, that processing is restricted or that the data is deleted. If the data subject considers that Avonova is processing personal data concerning him or her that are incorrect or incomplete, the data subject may request to have these corrected or supplemented.

The data subject also has the right to have their data deleted, including if they are no longer necessary or if the processing is based on consent and this has been revoked.

3.3.3. Right to object

The data subject has the right at any time to object to the processing of his/her personal data if the legal basis for the processing follows from GDPR Article 6 first paragraph letter e "public interest", or Article 6 first paragraph letter f "balancing of interests".

The above means, among other things, that the data subject has the right to object to the processing of their personal data for direct marketing.

If the individual objects to the processing, Avonova can only continue to process the data if it can be shown that there is a legitimate interest to the processing or if it is justified in storing the data for the purpose of establishing, exercising or defending legal claims.

3.3.4 Right to data portability

The data subject has the right to obtain the personal data he or she has provided to the controller and has the right to transmit these data to another controller. However, this applies provided that it is technically feasible and the legal basis for the processing consists of consent or that the processing has been necessary for the performance of a contract with the data subject.

3.3.5 Right to withdraw consent

If the processing of personal data is based on the data subject's consent, he or she has the right to withdraw this consent at any time. Such revocation does not affect the lawfulness of processing of personal data that took place before the consent was revoked.

3.3.6 How do we protect your personal data?

Your safety is important to us. Therefore, we have security measures in place to protect your personal data from unauthorized access and other unauthorized processing. We regularly analyse and evaluate the measures taken to ensure that the protection of your data is as secure as possible.

3.3.7 How long is personal data stored?

Avonova endeavours not to store more information than is necessary for the purposes. Relevant information is stored in accordance with current legislation.

3.4 Who do we disclose your data to?

We share your personal data with different recipients:

Service providers. In order to process personal data, we share personal data with service providers that we have engaged. For example, these service providers offer IT and communication services (which allow us to send you messages). When the service providers process personal data on our behalf and according to our instructions, they are data processors for us and we are responsible for the handling of your personal data. The service providers may not use your personal data for their own purposes and they are obliged by law and contract with us to protect your data.

Group companies. The companies in the Avonova Group cooperate with each other and therefore share information among themselves, for example in connection with communication. To the extent that group companies handle personal data on our behalf and in accordance with our instructions, for example to manage our relationship with customers, suppliers and partners, they are data processors for us and we are responsible for their handling of your personal data.

Your employer. Within the framework of a statutory duty of confidentiality, we may share personal data about you when we communicate with your employer (our customer), for example in connection with a case or inquiry.

Suppliers and partners. We may share your personal data with our partners and suppliers if it is necessary to fulfil our obligations and rights towards our customers.

Other recipients. In some cases, where necessary, we share your personal data with other recipients for certain purposes:

- to manage a merger or sale of our business,
- to manage and meet legal requirements,
- to fulfil legal obligations,
- to reply to an enquiry, and
- to protect and guarantee the security for our staff

Examples of recipients are external advisers, authorities, courts, the police and potential buyers or sellers if we were to sell the business.

4. Data security, controls and event management

To protect customers' data, Avonova uses security solutions from internationally recognized suppliers of the security industry. The solutions are configured according to industry practice. When using SaaS services, suppliers are selected who can demonstrate a commitment in line with internationally recognized standards and who are subject to GDPR. Avonova continuously evaluates its suppliers, partners and processes to ensure adequate security of our services.

4.1. Risk management

Our business always strives for continuous improvement, which is beneficial for our customers and our business. In order to be competitive, we work hard to look for opportunities where we can offer added value to our customers. However, these opportunities also involve risks that must be managed in order for us to fulfil our obligations to protect our customers' information. We work continuously with risk assessments in our operations and implement measures for preventive purposes. Therefore, we conduct risk and vulnerability analyses when introducing new solutions.

4.2 Breach management

Avonova works actively with incident management together with its operating partner to quickly resolve incidents and minimize impact for Avonova and our customers. Upon completion of the incident, Avonova learns from working preventively against future incidents. In the event of critical incidents, an incident report and a review of the lessons learned from the critical incident are established.

4.3 Access control

Protecting our customers' data against unauthorized access is of utmost importance to Avonova. We work with personal and access-controlled accounts, where each account has only the necessary rights (the principle of "least privilege") for us to be able to carry out our obligations.

4.4 Data security

At Avonova, we use encryption when transferring data over non-secure media and when data is at rest, based on the sensitivity and assessed risk of the information.

4.5 Change management

At Avonova, we work according to change processes with tests and test environments. Through controlled and tested changes, we ensure the security and availability of our services.

4.6 Impact assessment

Avonova works with impact assessments according to the Data Protection Regulation in the cases where the planned processing probably results in a high risk to natural persons' rights and freedoms. In the development or alternation of services, Avonova performs an assessment based on criteria in accordance with guidance from the supervisory authority to establish whether the processing, particularly with the use of new technology and taking into account its nature, scope, context and purpose, probably results in a high risk to natural persons' rights and freedoms and what risk reduction measures should be taken where applicable.

4.7 Transfer of personal data to third countries

We store our corporate customers' employees' personal data within the EU/EEA area. For customer relationship management, company information, as well as contact person and contact information will be stored in our CRM system HubSpot. This contact information is currently stored outside the EU/EEA area. For further information, see section 5.

5. Our core systems

In order to offer services within occupational health and management, Avonova uses a number of IT solutions. Our electronic health record system, which we use to keep medical records and make reservations, is central to providing services efficiently. Other key systems are our video consultation solution and our web portal. In this section, we will go through the technical interfaces you will encounter as a customer and contact person, as well as the central IT solutions we use to provide our services.

5.1 Safe zone

Safe Zone is a networked separated environment, a Citrix farm, and medical system and features. The goal of separation is to keep patient information secure and disconnected from the internet.

5.2 Customer portal

The Customer Portal is a web-based solution, where specific customer employees have the opportunity to log in with an assigned rights-controlled user account. The customer can view their orders and staff, as well as place new orders. The customer portal is presented through Episerver solution on our servers on prem at our operating partner. The information is displayed through APIs via a VPN tunnel. Data is stored only in the secure zone.

5.3 Avonova Digital

Avonova HR and HSE is an electronic tool for handling systematic HSE work for Avonova's customers. Avonova Digital is used for handling risk analyses, audits, nonconformities, safety inspections, secure job analysis, employee handbooks, holiday planning, absence, working hours, etc. Users authenticate via Avonova OneUser (IM) built on Azure AD B2C (OAuth/OpenID).

5.5 HubSpot

Cloud-based system for emination of the company's contact information, marketing and customer service. Data is stored encrypted and with access control through multifactor authentication. The system processes the stored personal data in accordance with European legislation.

5.6 FrontCore

Cloud-based system for administration and coordination, and delivery of course activities provided by Avonova. Data is stored encrypted with access control.

avonova

Detailed information on the processing of personal data

Please see below for detailed information on which categories of personal data we process, based on what legal basis and how long we store the data for each processing.

Purpose	*Personal data*	*Legal basis*	*Storage time*
Manage your relationship with customers	Order details Billing basis Identity data Communication Contact Profile information	*Legitimate interest*. The processing is necessary to satisfy our legitimate interest in managing our relationship with customers. *Fulfillment of contract*. If the agreement is entered into with a sole proprietorship, the processing takes place to fulfil the agreement with the sole proprietorship.	Personal data is stored for this purpose for as long as it is an active relationship and for a period of ten (10) years thereafter to satisfy our legitimate interest in handling and responding to legal claims.
Manage orders	• Order data • Invoicing data • Identity data • Contact details • Profile data • Communication	*Legitimate interest.* The processing is necessary to meet our legitimate interest in managing orders of products and services. *Fulfil contractual obligations.* If a contract has been entered into with a sole trader, the processing takes	Personal data are saved for this purpose for as long as necessary to manage the order and for a 10-year period afterwards to meet our legitimate interest in managing and meeting legal requirements.

		place to fulfil contractual obligations with the sole trader.	
Follow up and evaluate relationships with customers	• Order data • Identity data • Profile data	*Legitimate interest.* The processing is necessary to meet our legitimate interest in following up our relationship with our clients.	Personal data are saved for this purpose for 27 months starting from the time of data collection. Reports at overall level and statistics that do not include personal data are saved until further notice or until they are deleted.
Answer questions and provide customer service	• Order data • Identity data • Contact details • Profile data • Communication	*Legitimate interest.* The processing is necessary to meet our legitimate interest in answering your questions and providing customer service to our clients.	Personal data are saved for this purpose for six (6) months starting from the time when the case was concluded.
Newsletter	• Identity data • Contact details	*Legitimate interest.* The processing is necessary to meet our legitimate interest in sending our newsletter to you when you have subscribed to the newsletter.	Personal data are saved for this purpose until further notice and until you unsubscribe from the newsletter.
Follow up and evaluate the business	• Identity data • Order data • Profile data	*Legitimate interest.* The processing is necessary to meet our legitimate interest in following up and evaluating our activities.	Personal data are saved for this purpose for 27 months starting from the time of data collection. Reports at overall level that do not contain personal data and statistics are saved until

			further notice or until they are deleted.
Develop and improve operations	• Identity data • Order data • Profile data	*Legitimate interest.* The processing is necessary to meet our legitimate interest in developing and improving our activities.	Personal data are saved for this purpose for 27 months starting from the time of data collection. Reports and statistics at overall level that do not contain personal data are saved until further notice or until they are deleted.
Document our activities	• Audio and visual materials • Identity data • Communication • Contact details • Profile data	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in documenting our activities.	Personal data are saved for this purpose, as a starting point, until further notice.
Hold events and other activities	• Audio and visual materials • Identity data • Communication • Contact details • Profile data	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in holding the event or activity.	Personal data are saved for this purpose for the duration of the activity and for up to 13 months afterwards starting from the time when the activity was held in order to fulfil our legitimate interest in following up the participation and evaluating the activity as well as for planning possible future activities. Reports drawn up at overall level and statistics that do not contain personal data are saved until further notice or until they are deleted.
Conduct questionnaires	• Identity data • Communication • Contact details	*Legitimate interest.* The processing is necessary in order	Personal data are saved for this purpose for the duration of the survey and

	• Profile data	to fulfil our legitimate interest in conducting questionnaire-based surveys with the aim of compiling your opinions about our activities and services.	for three (3) months afterwards in order to compile the responses in a report. Reports at overall level that do not contain personal data and statistics are saved until further notice or until they are deleted.
Ensure technical functionality and security	• All affected categories of personal data.	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in ensuring necessary technical functionality and security in our IT systems.	Personal data are saved during the same period as stated in relation to each affected purpose of the processing. Personal data in logs are saved for troubleshooting and breach management for 13 months starting from the time of the log event. Personal data in backups are saved for 13 months starting from the time of the backup.
Manage and meet legal requirements	• Affected categories of personal data that are necessary in order to manage and meet the legal requirement in the individual case.	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in managing and meeting legal requirements.	Personal data are saved for this purpose for the length of time necessary to manage the legal requirement in the individual case.
Fulfil legal obligations	• Affected categories of personal data that are necessary to	*Fulfil legal obligations.* The processing is necessary in order	Personal data are saved for the time necessary to enable us to fulfil our respective legal obligations. For example, personal data

	fulfil each legal obligation.	to fulfil our legal obligations.	in accounting material are saved for ten (10) years starting from the end of the calendar year when the relevant financial year ended.

When we share personal data

Please see below for detailed information on which categories of personal data we share with different categories of recipients for different purposes and on what legal basis.

Receiver	***Purpose***	***Personal data***	***Legal basis***
Group company	Communication between employees at various Avonova companies with the aim of managing our relationship with our clients, for example, in order to provide our services.	• Invoicing data • Identity data • Communication • Contact details • Profile data	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in various Avonova companies being able to manage our relationship with our clients, for example, to provide our services.
Suppliers and partners	Fulfil our obligations and rights in relation to our client companies, for example, to provide our services with the help of partners.	• Identity data • Communication • Contact details • Profile data	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in bring able to fulfil our obligations and rights in relation to our client companies.
Your employer	Fulfil our rights and obligations in relation to our client companies (your employer),	• Identity data • Communication • Contact details Profile data	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in bring able to

	for example, to provide our services and reply to enquiries.		fulfil our obligations and rights in relation to our client companies.

Other recipients

Purpose	***Legal basis***
Manage a merger or sale of the business Only necessary personal data are shared with the recipient for this purpose.	*Legitimate interest.* The processing is necessary in order to fulfil our and the buyer's legitimate interest in implementing the merger or sale.
Manage and meet legal requirements Only the categories of personal data that are necessary in order to manage and meet the legal requirement in the individual case.	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in managing and meeting legal requirements.
Fulfil legal obligations Only the categories of personal data that are necessary to fulfil each respective legal obligation.	*Fulfil legal obligations.* The processing is necessary in order to fulfil our legal obligations.
Reply to an enquiry Only the categories of personal data that are necessary in order to reply to an enquiry.	*Legitimate interest* or *fulfil a legal obligation*. To the extent that we are obliged to reply to an enquiry, personal data is processed to fulfil the legal obligation. The processing otherwise takes place supported by a legitimate interest assessment when necessary in order to fulfil our and the questioner's legitimate interest in us replying to the enquiry.
Protect and guarantee security for our staff. Only the categories of personal data that are necessary for this purpose, for	*Legitimate interest.* The processing is necessary in order to fulfil our legitimate interest in protecting and guaranteeing security for our staff.

example, to report a breach to a law enforcement authority.	