

Privacy policy for Avonova's customer



Version 1.1

23-12-05

Head office

Avonova Hälsa AB
556500-6821

Klarasbergsviadukten 90
11164 Stockholm, Sweden

kontakt@avonova.se

Data protection officer

gdpr@avonova.se



Contents

List of terms	4
1. Introduction to Avonova	7
1.1 Avonova's service offering	7
1.2 The aim of this policy	7
2. Avonova's responsibility and obligations	8
2.1 Avonova's principles about personal data	8
2.2 Personal data responsibility	8
3. The processing of personal data	9
3.1 Where do we collect personal data from?	9
3.2 Why do we process your personal data?	9
3.3 Rights	12
4.4 Who do we supply your data to?	14
4. Data security, controls and breach management	15
4.1 Risk management	15
4.2 Breach management	15
4.3 Access control	15
4.4 Data security	16
4.5 Change management	16
4.6 Impact assessment	16
4.7 Transfer of personal data to a third country	16
5. Our core systems	17
5.1 CompuGroup Medical Journal 4 (CGMJ4)	17
5.2 Avonova's web portal	17
5.3 Aurora TeleQ	18
5.4 Avonova Säkert Möte (secure meeting)	18



Detailed information on the processing of personal data	19
When we share personal data.....	24



List of terms

In addition to the terms defined in running text, the following definitions shall apply, regardless of whether they are used in the plural, singular, definite or indefinite forms.

Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data protection legislation	Refers to all integrity legislation and personal data legislation, as well as any other legislation (including regulations and provisions), which is applicable to the personal data processing that takes place according to this integrity and data security policy, including EU legislation and legislation in EU Member States.
Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Instruction	The written instructions that detail the subject matter, duration, nature and purpose, type of personal data and categories of data subjects and special needs encompassed by the processing.
Contact person	An employee who works at a company, public authority or organisation that is one of Avonova's clients and who is Avonova's contact person or otherwise has contact with us about issues concerning the relationship between Avonova and the client company.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Personal data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.



Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data that have been transmitted, stored or otherwise processed.
Data subject	Natural person whose personal data are processed.
Third country	A state that is not included in the European Union (EU) or is not a party to the European Economic Area (EEA).
Sub-processor	Natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the processor, processes personal data on behalf of the controller.
Healthcare provider	Healthcare provider refers to a government authority, county council or municipality in matters of such healthcare for which the authority, county council or municipality is responsible and other legal person or sole trader that runs healthcare, according to the Swedish Patient Safety Act (2010:659), Chapter 1, Section 3.
The Swedish Patient Safety Act (Patientsäkerhetslag, 2010:659)	In this Act, patient safety means protection against healthcare injury.
The Swedish Patient Data Act (Patientdatalagen, 2008:355)	The rules for processing personal data in healthcare are stated in the Patient Data Act. All healthcare providers, both those under public management and those under private management, shall apply the Patient Data Act.
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 about your profile, such as your title and the name and address of the company or organisation that 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's service offering

Avonova offers services in the areas of occupational health and leader development. With a wide range of knowledge and extensive commitment, we help organisations and their employees become more sustainable, communicate more effectively and feel better. Our employees deliver health services throughout Sweden every day.

Under 'Avonova tjänster' on our website, we have compiled information on everything we offer our clients to help develop health and work environment management to a sustainable level. We offer services focusing on the development and systematics of health work and work-environment management. <https://www.avonova.se/tjanster/>

Avonova is third-party certified through Qvalify within ISO 9001:2015 (quality), ISO 14001:2015 (environment), ISO 45001:2018 (work environment) and Krav – a management system for quality within Swedish occupational health services, edition 7/2016-02.

Our enterprise resource planning (ERP) system describes how, in the fields of quality, environment and work environment, we verify our activities, perform our services, fulfil requirements and criteria, and handle improvement and deviation management. Avonova is a member of Sveriges Företagshälsor, an occupational health industry association and follows its guidelines.

Through these systems, we can guarantee that our staff have qualifications that comply with the industry's guidelines, perform services and apply methods and techniques that are based on objectivity, science and proven experience.

1.2 The aim of this policy

Avonova cares about your integrity and has, therefore, drawn up this policy. It is based on applicable data protection legislation. It clarifies how Avonova endeavours to safeguard your rights and integrity. In Sweden, the processing of personal data is regulated by the EU's General Data Protection Regulation (the Data Protection Regulation or GDPR) and the complementary Swedish Data Protection Act (2018:218). For healthcare providers, there are also supplementary provisions in the Patient Data Act (2008:355). All of the three regulatory frameworks therefore apply to Avonova.

This policy aims to inform you how Avonova works and how we process your personal data, what we use them for, who has permission to access them, and how you can safeguard your rights when you are a contact person and have contact with us.



2. Avonova's responsibility and obligations

2.1 Avonova's principles about 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 Personal data responsibility

According to the Work Environment Act, occupational health care must work in particular to prevent and eliminate health risks at workplaces and have the competence to identify and describe the connections between the work environment, organization, productivity and health.

Operations at Avonova according to the Health and Medical Care Act (2017:30) means that Avonova is the personal data controller according to ch. 2. Section 6 of the Patient Data Act (SFS 2008:355), not only for purposes that intend to keep patient records according to ch. 3. the patient data act, but also when Avonova prepares other documentation that is needed in and for the care of patients and administration that concerns patients and that aims to provide care in individual cases or is otherwise prompted by care in individual cases.

The processing of personal data is necessary to satisfy our legitimate interest (Article 6.1 F) in being able to provide services to you as a customer and you as an employer's legitimate interest in being able to provide services to your employees as part of the systematic work environment work.

When the customer has contact with Avonova in various contexts, Avonova's handling of personal data is covered by both the GDPR and the Patient Data Act (2008:355). Personal data is processed by Avonova within the healthcare system if necessary for:

- (i) to fulfill obligations to establish documentation needed in and for the care of patients;
- (ii) administration relating to patients and which is aimed at providing care in individual cases or which is otherwise prompted by care in individual cases,



(iii) to prepare other documentation that follows from law, regulation or other constitution,
(iv) to systematically and continuously develop and secure the quality of the business,

(iv) administration, planning, follow-up, evaluation and supervision of the business, and

(v) to produce statistics on healthcare.

2.3 Data Processor

Avonova Solutions AS is the data processor for its customers who use the system Avonova Digital and SAM Digital.

3. The processing of personal data

3.1 Where do we collect personal data from?

We collect personal data from:

- Your employer (name, address, e-mail address and organisational category/group/department)
- You (for example, when you communicate with us by e-mail)
- From other companies in the Avonova group (for example, name and e-mail address)
- From public registers (for example, if you are an authorised signatory, managing director or board member of a company that is one of Avonova's clients)

3.2 Why do we process your personal data?

Introduction

Below we list more detailed information about why we use your personal data in various cases. To read more about which categories of data are saved, which legal basis supports our use of personal data for each purpose and how long your personal data are saved, see **our detailed information about processing personal data** further on in this document.



Manage our relationship with clients, suppliers and partners

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

Manage orders

To manage orders of services from clients, where applicable, we use your personal data when you are the contact person for this purpose, for example, to manage order confirmations and communicate with you regarding the order.

Follow up and evaluate our relationship with clients

We use your personal data as a contact person when necessary in order to follow up and evaluate our client relationship.

Answer questions and provide customer service

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

Communication between our employees and external people in the service

Where applicable, we handle your personal data in connection with communication, for example, through e-mail, between our employees and external people.



Provide newsletters

We use your personal data to provide our newsletter, for example, to register your subscription to the newsletter and to send the newsletter to you. You can unsubscribe from mailings at any time by clicking on the unsubscribe link in the e-mail or by contacting us.

Follow up and evaluate our activities

We use your personal data to compile reports at an overall level and statistics in order to follow up and evaluate our activities.

Develop and improve our activities

We use your personal data when we conduct overall analyses to develop and improve our activities, business methods and business strategies.

Document our activities

We use your data where applicable to document our activities, for example, to manage and save contracts, data forming a basis for decisions, minutes of meetings and presentations.

Hold events and other activities

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

Conduct questionnaires

If you choose to take part in a questionnaire-based survey that we conduct, we collect the personal data that you submit in connection with the questionnaire. Your opinions about our activities and services are important to us. You can unsubscribe from mailings at any time by clicking on the unsubscribe link in the e-mail or by contacting us.

Ensure technical functionality and security

We use your personal data to ensure necessary technical functionality and security in our IT systems, such as in security logging, error management and backups.

Manage and meet legal requirements



We process your personal data if this is necessary to manage and fulfil a legal requirement, for example, in conjunction with a dispute or a lawsuit. For this purpose, we may share some information with other recipients; see further on in this document for more details.

Fulfil legal obligations

In order to fulfil our legal obligations, when necessary, we manage your personal data, for example, to comply with legislation in the fields of healthcare, accounting or data protection. For this purpose, we may share some information with other recipients; see further on in this document for more details.

3.3 Rights

3.3.1 Right to access

The data subject has the right to contact Avonova, who is the controller, and request access to the personal data that Avonova holds and information such as the purposes of the processing of that information and which personal data have been shared.

In the role of controller, Avonova shall provide the data subject with a free copy of the personal data that they hold. If extra copies are requested, Avonova may charge an administration fee.

3.3.2 Right to correction, erasure or restriction

The data subject has the right, without undue delay, to have their personal data corrected or, in certain circumstances, to have the processing limited or the data deleted. If the data subject is of the opinion that Avonova is processing personal data about them that is incorrect or incomplete, the data subject has the right to demand correction or supplementation of these data.

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



3.3.3 Right to object

The data subject has the right to object at any time to the processing of their personal data if the legal basis for the processing relates to Article 6.1 (e) 'allmänt intresse' (public interest) or 6.1 (f) 'intresseavvägning' (legitimate interest assessment) in the Data Protection Regulation.

The above means 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 may only continue to process the data if it can be demonstrated that there are compelling legitimate grounds for the processing or if it is justifiable to store the data to enable the establishment, exercise or defence of legal claims.

3.3.4 Right to data portability

The data subject has the right to obtain the personal data that they have provided to the controller and has the right to transfer these data to a different controller. However, this only applies if it is technically possible and consent is the legal basis for the processing or that the processing has been necessary to fulfil contractual obligations with the data subject.

3.3.5 Right to withdraw consent

If the processing of the personal data is based on the consent of the data subject, the latter has the right to withdraw their consent at any time. Such withdrawal does not affect the legality of personal data processing that took place before the consent was withdrawn.

3.3.6 How do we protect your personal data?

Your security is important to us, which is why we have security measures in place to protect your personal data from unauthorised access and other unlawful processing. We regularly analyse and evaluate these measures to ensure that the protection of your data is as secure as possible.

3.3.7 How long are your personal data stored for?

Avonova endeavours not to store more information than necessary for the purposes set out and according to stipulations in national legislation, such as Bokföringslagen (the Swedish Book-keeping Act, 1999:1078). See below for more details.



4.4 Who do we supply your data to?

We share your personal data with various recipients:

Service providers. In order to manage personal data, we share such data with service providers who we have engaged. For example, those providing IT and communication services (enabling us to send messages to you). When the service providers process personal data on our behalf and according to our instructions, they are our processors and we are responsible for the management of your personal data. The service providers are not permitted to use your personal data for their own purposes, and they are obliged by legislation and through their contracts with us to protect your data.

Group companies. The companies in the Avonova group collaborate with each other and, therefore, share data with each other, for example, in conjunction with communication. To the extent that group companies manage personal data on our behalf and according to our instructions, for example, to manage the relationship with clients, suppliers and partners, they are our processors and we are responsible for their management of your personal data.

Your employer. We share personal data about you when we communicate with your employer (our client), such as within the framework of a case or enquiry.

Suppliers and partners. We may share your personal data with our partners and suppliers if this is necessary to fulfil our obligations and rights in relation to our clients.

Other recipients. In certain 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 such recipients are external advisors, authorities, courts of law, the police and potential buyers or sellers if we were going to sell the business.



4. Data security, controls and breach management

To protect our clients' data, Avonova uses security solutions from internationally well-known suppliers in the security industry. The solutions are configured according to industry practice and placed with Avonova's ISO-27001-certified operating partner in Sweden. When using SaaS services, suppliers that demonstrate a commitment in line with internationally recognised standards (ISO-27001 or similar) and that are governed by GDPR are selected. Avonova continually evaluates its suppliers, partners and processes to ensure satisfactory security for our services.

4.1 Risk management

We endeavour to constantly improve our activities, which benefits our clients and our organisation. To be competitive, we extensively search for opportunities to offer added value to our clients. However, these opportunities also entail risks that must be managed in order for us to uphold our commitment to protect our clients' information. We continually work with risk assessments in our activities and take preventive action. We, therefore, perform risk and vulnerability analyses in conjunction with the implementation of new solutions.

4.2 Breach management

Avonova works actively with breach management together with its operating partner to rapidly resolve breaches and minimise the impact on Avonova and its clients. After a breach has occurred, Avonova takes note of any lessons learnt to proactively prevent future breaches. In critical breaches, an incident report is written, and the incident is reviewed in a lessons-learnt session.

4.3 Access control

Protecting our clients' information from unauthorised access is of utmost importance to us at Avonova. We work with personal accounts, each of which only has the necessary rights (the 'least privilege' principle) to enable us to fulfil our commitments.



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. We use verified and tested changes to 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 a third country

We always endeavour to save personal data within the EU. In certain cases, your personal data is shared with recipients outside the EU/EEA, such as service providers who we have engaged.

To ensure that the personal data are protected, we make sure that suitable protection measures are in place at all service providers who manage your personal data outside the EU/EEA in light of the recipient country's legislation. In cases of third-party transfers Avonova always concludes data transfer agreements that include standard clauses for transferring personal data.

If you would like more detailed information about which countries outside the EU/EEA we transfer your personal data to and what protection measures we have taken to protect your personal data, please contact us; see the first page for contact details.



5. Our core systems

Avonova uses a series of IT solutions in order to offer occupational health services and leadership services. Our electronic patient record system, into which we write patient records and enter bookings, is central to our ability to offer services efficiently. Other core systems consist of our video consultation solution and our web portal. In this section, we will go through the technical interfaces you will encounter as a client and contact person, as well as the central IT solutions that we use to offer our services.

5.1 CompuGroup Medical Journal 4 (CGMJ4)

Avonova uses CGMJ4 as an electronic patient record and booking system. The system comprises the patient records, client portal and online appointment booking service.

- Patient records
The system processes our patient records and is governed by the Swedish Patient Data Act SFS 2008:355, the Swedish Patient Safety Act SFS 2010:659, and the National Board of Health and Welfare's provisions and general guidelines (HSLF-FS 2016:40) concerning patient records and processing of personal data within health and medical care. The patient record database is encrypted and is hosted within Sweden at our operating partner.
- Client portal (invoicing data)
The client portal is used for the publication of details for invoicing and includes these data: invoicing data, basic data for Hälsocenter (healthcare centres), personal basic data and sensitive personal data. Data are transferred from the patient record system to the invoicing portal to be made available for each recipient of the invoicing data.
- Online appointment booking service
Avonova's 'webbtidbok' is an online service integrated into Avonova's patient record and booking system CGMJ4, enabling our clients such as purchasers/contact persons and client employees to book appointments for themselves at reserved times. The transfer of data between the client portal, appointment booking service and the CGMJ4 patient record system to generate appointment times in the patient record system's booking module takes place via HTTPS with TLS 1.2 encryption standard.

5.2 Avonova's web portal

Avonova's web portal is used for ordering services, communication with purchasers/contact persons, file sharing, news publication, etc. The portal is based on a Sharepoint solution. Also



see <https://www.avonova.se/gdpr/>

5.3 Aurora TeleQ

Cloud-based communication solution for managing incoming calls with a phone button-based menu for case management based on Avonova's division into areas, where queue management and a callback function are included. The supplier manages the login and verification.

5.4 Avonova Säkert Möte (secure meeting)

Avonova 'Säkert Möte' is a secure meeting tool for consultations between healthcare providers and client employees. All infrastructure is located in Sweden. Clients verify their identity using the BankID app and Avonova's staff verify their identity using personal accounts.



Detailed information on the processing of personal data

See below for detailed information on which categories of personal data we process, on what legal basis and how long we save the data for each processing.

Purpose	Personal data	Legal basis	Storage period
Manage our relationship with clients	<ul style="list-style-type: none"> • Order data • Invoicing data • Identity data • Communication • Contact details • Profile data 	<p><i>Legitimate interest.</i> The processing is necessary to meet our legitimate interest in managing our relationship with clients.</p> <p><i>Fulfil contractual obligations.</i> If a contract has been entered into with a sole trader, the processing takes place to fulfil contractual obligations with the sole trader.</p>	Personal data are saved for this purpose for the duration of the active relationship and for a 10-year period afterwards to meet our legitimate interest in managing and meeting legal requirements.
Manage orders	<ul style="list-style-type: none"> • Order data • Invoicing data • Identity data • Contact details • Profile data • Communication 	<p><i>Legitimate interest.</i> The processing is necessary to meet our legitimate interest in managing orders of products and services.</p> <p><i>Fulfil contractual obligations.</i> If a contract has been entered into with a sole trader, the processing takes</p>	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 our relationship with clients	<ul style="list-style-type: none"> • Order data • Identity data • Profile data 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> • Order data • Identity data • Contact details • Profile data • Communication 	<i>Legitimate interest.</i> 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.
Provide newsletters	<ul style="list-style-type: none"> • Identity data • Contact details 	<i>Legitimate interest.</i> 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 our activities	<ul style="list-style-type: none"> • Identity data • Order data • Profile data 	<i>Legitimate interest.</i> The processing is necessary to meet our legitimate interest in following	Personal data are saved for this purpose for 27 months starting from the time of data



		up and evaluating our activities.	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 our activities	<ul style="list-style-type: none"> • Identity data • Order data • Profile data 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> • Audio and visual materials • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> • Audio and visual materials • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> The processing is necessary in order to fulfil our legitimate interest in conducting questionnaire-based surveys with the aim of compiling your opinions about our activities and services.	Personal data are saved for this purpose for the duration of the survey and 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	<ul style="list-style-type: none"> • All affected categories of personal data. 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> Affected categories of personal data that are necessary in order to manage and meet the legal requirement in the individual case. 	<i>Legitimate interest.</i> 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	<ul style="list-style-type: none"> Affected categories of personal data that are necessary to fulfil each legal obligation. 	<i>Fulfil legal obligations.</i> The processing is necessary in order to fulfil our legal obligations.	Personal data are saved for the time necessary to enable us to fulfil our respective legal obligations. For example, personal data in accounting material are saved for seven (7) years starting from the end of the calendar year when the relevant financial year ended according to the Swedish Book-keeping Act (1999:1078).



When we share personal data

See below for detailed information on which personal data categories we share with various recipient categories for various purposes and which legal basis supports this.

Recipient	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.	<ul style="list-style-type: none"> • Invoicing data • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> 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.	<ul style="list-style-type: none"> • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> 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), for example, to provide our services and reply to enquiries.	<ul style="list-style-type: none"> • Identity data • Communication • Contact details • Profile data 	<i>Legitimate interest.</i> 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.



Other recipients

Purpose	Legal basis
<p><i>Manage a merger or sale of the business</i></p> <p>Only necessary personal data are shared with the recipient for this purpose.</p>	<p><i>Legitimate interest.</i> The processing is necessary in order to fulfil our and the buyer's legitimate interest in implementing the merger or sale.</p>
<p><i>Manage and meet legal requirements</i></p> <p>Only the categories of personal data that are necessary in order to manage and meet the legal requirement in the individual case.</p>	<p><i>Legitimate interest.</i> The processing is necessary in order to fulfil our legitimate interest in managing and meeting legal requirements.</p>
<p><i>Fulfil legal obligations</i></p> <p>Only the categories of personal data that are necessary to fulfil each respective legal obligation.</p>	<p><i>Fulfil legal obligations.</i> The processing is necessary in order to fulfil our legal obligations.</p>
<p><i>Reply to an enquiry</i></p> <p>Only the categories of personal data that are necessary in order to reply to an enquiry.</p>	<p><i>Legitimate interest or fulfil a legal obligation.</i> 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.</p>
<p><i>Protect and guarantee security for our staff.</i></p> <p>Only the categories of personal data that are necessary for this purpose, for example, to report a breach to a law enforcement authority.</p>	<p><i>Legitimate interest.</i> The processing is necessary in order to fulfil our legitimate interest in protecting and guaranteeing security for our staff.</p>

