



Privacy Notice

How we process and protect personal data

Version 1.0 | Last updated 2 September 2026

In brief. We use personal data only for clear and lawful purposes, limit access to those who need the data for their work, and give special protection to client and health data. We never sell personal data.

This notice provides Aurora Care Oy's general information on personal data processing under Articles 12–14 of the EU General Data Protection Regulation. Additional information may be provided for specific services or records.

1. Who is responsible for the data?

Controller: Aurora Care Oy, Business ID 3287707-7

Address: Jeansborgintie 1 A, FI-66900 Uusikaarlepyy, Finland

Email: info@auroracare.fi | Website: www.auroracare.fi

Data Protection Officer: Johanna Frostdahl. Contact her at info@auroracare.fi and use "Data protection matter" as the subject line.

When a service is arranged by a wellbeing services county, the county is normally the controller of client data generated in publicly arranged social welfare. Aurora Care then processes the data on behalf of the county and in accordance with its instructions. When a client purchases a private service directly from Aurora Care, or when the processing concerns Aurora Care's own personnel, finance, communications or patient administration, Aurora Care is normally the controller.

2. Whose data do we process?

- clients and patients, as well as their legal representatives, close relatives and contact persons
- employees, trainees, job applicants and former employees
- commissioning parties, contractual partners, authority contacts and other partners
- people who contact us, provide feedback or respond to a survey

Fully anonymous survey responses are not personal data. We design our client and staff surveys so that individuals cannot be identified in the reporting.

3. What data may we process?

- **Basic and contact data:** name, personal identity code when necessary, address, telephone number, email address, language and contact persons.
- **Client and patient data:** service and care needs, functional capacity, care and service plans, medication data, records, decisions and information needed for safe care and support.
- **Financial and contractual data:** invoicing, payments, contracts, service decisions and other information required for administration and statutory accounting.
- **Personnel data:** employment, working hours, shifts, salary, qualifications, training, occupational healthcare and other information required by the employer under law.

- **Communications and technical data:** messages, feedback, consents, user and log data, and data necessary for the use of our digital services.

4. Why and on what grounds do we process data?

We process data to arrange and provide safe care, support, medical services and other agreed services; document and monitor services; manage client and patient safety, medication safety, quality, invoicing, accounting, personnel administration, authority contacts and feedback; protect our systems; and investigate incidents.

Depending on the situation, the legal basis is a contract, a legal obligation, a task carried out in the public interest, Aurora Care's legitimate interest or consent. Sensitive client, health and personnel data are processed only where there is a specific basis under Article 9 of the GDPR and applicable Finnish law, particularly for the provision of social and healthcare services or compliance with the employer's legal obligations. Consent is used mainly for voluntary purposes and may be withdrawn.

Our legitimate interests primarily include managing appropriate communications, protecting people, operations and information systems, preventing misuse, and establishing or defending legal claims. Data required by law or contract are mandatory; without them, we may be unable to provide the service, enter into or perform a contract, or handle the matter.

5. Where do we obtain the data?

Data are obtained primarily from the individual or their legal representative. We may also obtain necessary data from an authorised close relative, a wellbeing services county or other commissioning party, previous care and service units, the Kanta Services, competent authorities, professionals and other lawful sources. Personnel data are mainly obtained from the employee and from authorities or service providers used by the employer under law.

6. What systems do we use?

Our main systems are DomaCare for client and care data, Diarium for patient data at the medical clinic, Netvisor for financial administration, and Työvuorovelho for working time and shift planning. We also use secure email and other necessary communications and support services. System suppliers may process data only under contract and documented instructions.

7. Who may receive the data?

Only authorised persons may access the data, and only to the extent required by their duties. Data may be disclosed to the wellbeing services county, Kanta Services, competent authorities, care and service providers, laboratories, pharmacies, insurance and pension bodies, payroll and financial administration, auditors, and IT and other service providers where there is a lawful basis or valid consent.

We do not disclose data for another party's marketing and do not sell personal data. Data are processed primarily within the EU/EEA. If a technical supplier needs to process data outside the EU/EEA, a lawful transfer mechanism and appropriate safeguards under the GDPR are used. Further information on the transfer mechanism and safeguards is available from our data protection contact.

8. How long do we retain the data?

- Client and patient records are retained in accordance with the Act on the Processing of Client Data in Healthcare and Social Welfare, applicable authority regulations and the national retention periods of the Kanta Services.
- Accounting, payroll and contract material is retained for as long as required by accounting, tax, employment and limitation legislation or as needed to handle legal claims.
- Recruitment data are generally retained for no more than two years after the recruitment process ends, unless longer retention has been expressly agreed or is necessary for handling a legal claim.

- Contact and feedback data are retained only for as long as the matter requires, generally no more than two years after the matter is closed. Security and access logs are retained in accordance with law, security needs and a documented retention plan.

When data are no longer needed, they are erased, anonymised or archived lawfully. Aurora Care follows a documented retention and disposal plan.

9. How do we protect the data?

We use personal user accounts, role-based access rights, logging and monitoring, confidentiality commitments, training, backups, technical safeguards and written agreements with suppliers. Paper records are kept in locked premises. Suspected personal data breaches are investigated without delay and reported when required by law.

10. Your rights

Depending on the legal basis, you may have the right to:

- receive information about the processing and a copy of your personal data
- request the correction of inaccurate or incomplete data
- request erasure or restriction of processing where permitted by law
- object to processing based on legitimate interests or direct marketing
- receive your data in a portable form where processing is automated and based on a contract or consent
- withdraw consent without affecting the lawfulness of processing carried out before withdrawal

The right to erasure does not normally apply to client and patient records that must be retained by law. If the wellbeing services county is the controller, the request should be addressed to the county; Aurora Care will assist in forwarding the request where necessary. We may need to verify your identity before processing a request.

Send your request to info@auroracare.fi or by post to Aurora Care Oy. You also have the right to lodge a complaint with the Office of the Data Protection Ombudsman.

11. Automated decisions and updates

Aurora Care does not make decisions based solely on automated processing that produce legal or similarly significant effects for an individual. We update this notice when our operations, systems or legislation change. The current version will be available on our website and from Aurora Care.

Legal framework and further information

- [EU General Data Protection Regulation \(EU\) 2016/679](#)
- [Data Protection Act 1050/2018](#)
- [Act on the Processing of Client Data in Healthcare and Social Welfare 703/2023](#)
- [Act on the Protection of Privacy in Working Life 759/2004](#)
- [Office of the Data Protection Ombudsman](#)

Practical note. This general notice supplements, but does not replace, Aurora Care's internal record of processing activities, information security plan, retention and disposal plan, data processing agreements or register-specific instructions.