

# Privacy Notice

## Who we are

Caldora Compliance Limited operates the Caldora Compliance platform, a software-as-a-service tool that helps heat network operators and suppliers manage their regulatory compliance obligations. Our platform is accessible at [caldoracompliance.co.uk](http://caldoracompliance.co.uk).

We are registered in England and Wales under company number 17080432 and act as the data controller for the personal data described in this notice. This means we decide how and why that data is processed, and we are accountable for it under UK data protection law.

You can reach us at any time by emailing [info@caldoracompliance.co.uk](mailto:info@caldoracompliance.co.uk).

## What this notice covers

This notice sets out how we handle personal data in connection with operating our business. It covers people who visit our website, prospective and current customers, industry contacts, job applicants, and suppliers.

It does not cover personal data processed inside the Caldora Compliance platform on behalf of our customers, for example, the names of staff assigned to compliance tasks, or records of vulnerable or PSR customers entered by heat network operators. That processing is governed by a separate Data Processing Agreement, available on request, in which we act as a data processor on our customers' instructions.

## What we collect and why

The points below summarise the different groups of people whose data we may hold, the data we collect, our purpose, and our legal basis for processing it.

**Website and email enquiries.** When you contact us through our website or directly by email, we collect your name, email address and the content of your message. We use this to respond to your enquiry and to follow up where relevant. Our legal basis is our legitimate interest in communicating with people who reach out to us about our services. We keep this data only for as long as the interaction remains live or relevant.

**Platform users.** If you have an account on the Caldora Compliance platform, we hold your name, email address and role. We use this to authenticate your access, send you platform-related communications (including account invitations, password resets, weekly compliance summaries and billing notifications), and to maintain a secure, personalised experience. Processing is necessary to deliver the service under our contract with your organisation. We retain this data for the duration of your account and delete it within 30 days of account closure.

**Customer and partner contacts.** We may hold the name, job title, employer and contact details of people who work for our customers, partners or other organisations in the heat network sector. This data helps us to manage our commercial relationships and deliver our services effectively. We receive it directly from the individuals concerned, from their employers, or occasionally from publicly available professional sources. We process it on the basis of our legitimate interest in maintaining productive working relationships and retain it for as long as the relationship is active.

**Suppliers.** For the suppliers and contractors we work with, we hold contact details and any personal information needed to manage procurement and payments. This is processed on the basis of our legitimate interest in running our business operations efficiently.

**Job applicants.** If you apply to work with us, we will process the information you submit (typically your name, contact details and CV) to assess your suitability and to communicate with you about your application. We rely on our legitimate interest in identifying and recruiting suitable people. Applications from unsuccessful candidates are deleted within 12 months of a final decision.

### **Cookies**

Our platform uses strictly necessary session cookies to keep you securely logged in. These are essential to the service and do not require your consent. We do not use advertising cookies or behavioural tracking tools.

Our public website may use basic analytics to help us understand how visitors navigate the site. These cookies are set only where required consents are in place. You can manage cookie preferences through your browser settings.

### **How long we keep your data**

We do not hold personal data for longer than is necessary. Retention periods vary depending on the type of data and the purpose for which it was collected:

- Platform account data is kept for the duration of your account and deleted within 30 days of closure
- Enquiry and correspondence data is kept for as long as the interaction is live, and reviewed periodically thereafter
- Job application data for unsuccessful candidates is deleted within 12 months of a final decision
- Supplier and financial records may be retained for up to 7 years to meet statutory accounting requirements
- Where we are required by law or regulation to retain data for a specified period, we follow that requirement

## Who we share your data with

We do not sell personal data and we do not use it for advertising. We share data only where necessary:

- With our technology service providers, who process data on our behalf to operate the platform and run our business (see below)
- With professional advisers such as our lawyers, accountants or auditors, where they need access to provide their services
- With regulatory or law enforcement authorities, where we are required to do so by law

In the event of a business acquisition, merger or restructuring, personal data may be transferred to a successor entity. We would require that entity to honour the commitments in this notice.

**Technology providers.** We rely on a small number of specialist cloud service providers to operate our platform. These include providers of database hosting, file storage, transactional email, AI document processing, and payment infrastructure. Each provider acts as a data processor under a written agreement that restricts them from using your data for any purpose other than providing their service to us. We regularly review these arrangements to ensure appropriate safeguards are in place. If you would like details of specific providers or the data they process, please contact us.

## International data transfers

Our primary data infrastructure is located within the UK and European Economic Area. We store files on AWS S3 servers in Stockholm (EU North 1), and our database runs on infrastructure within the EEA.

Some of our service providers operate globally, and personal data may be processed on their infrastructure outside the UK or EEA. Where this happens, we ensure that an appropriate transfer mechanism is in place such as UK International Data Transfer Agreements or Standard Contractual Clauses. If you would like more information about how a specific provider handles international transfers, please get in touch.

## Your rights

UK data protection law gives you a number of rights in relation to your personal data. You can:

- Ask us for a copy of the personal data we hold about you (a subject access request)
- Ask us to correct personal data that is inaccurate or incomplete
- Ask us to delete your personal data, in certain circumstances
- Ask us to restrict how we use your data while a complaint or query is being resolved

- Object to processing that is based on our legitimate interests, where you feel it affects your fundamental rights
- Ask us to transfer your data to you or another provider in a portable format, where technically feasible
- Withdraw consent at any time where we rely on consent as our legal basis

To exercise any of these rights, email us at [info@caldoracompliance.co.uk](mailto:info@caldoracompliance.co.uk). We will respond within one calendar month. We will not charge a fee for reasonable requests.

### **Automated processing and AI**

We do not use personal data to make automated decisions that have a legal or similarly significant effect on any individual.

The Caldora Compliance platform includes AI-powered features that help users draft compliance documents and review evidence. These tools process the data users submit and return suggestions to assist with compliance tasks. All outputs are recommendations only, no automated decision replaces human judgement, and users remain fully responsible for the actions they take within the platform.

### **How we protect your data**

We apply technical and organisational security measures proportionate to the risk. These include encrypted data transmission over HTTPS, bcrypt hashing for passwords, server-side encryption for stored files, and role-based access controls within the platform to limit who can see what.

Access to personal data within our organisation is restricted to people who need it to do their job, and all such individuals are subject to confidentiality obligations.

If we become aware of a personal data breach that is likely to create a risk to individuals, we will notify the ICO within 72 hours and, where required, inform affected individuals without undue delay.

### **Questions and complaints**

If you have a question about this notice or the way we handle personal data, please email us at [info@caldoracompliance.co.uk](mailto:info@caldoracompliance.co.uk). We will do our best to resolve your concern promptly.

If you are not satisfied with our response, or if you believe we are processing your data unlawfully, you have the right to complain to the UK Information Commissioner's Office. You can reach the ICO at [ico.org.uk/concerns](https://ico.org.uk/concerns) or by calling 0303 123 1113.

### **Updates to this notice**

We review this notice periodically and update it when our practices change or when required by law. Where an update is material, we will let registered users know by email before the change takes effect. The version on our website at [caldoracompliance.co.uk/privacy](https://caldoracompliance.co.uk/privacy) is always the current one.