PRIVACY POLICY FOR VENTHERM A/S

Last updated: 25.04.2024

Data Controller

We are the data controller for the processing of personal data concerning our customers and business partners. Our contact details are as follows:

Company Name: VENTHERM A/S
Address: Kastanievej 5, 5672 Broby
CVR Number: 79219118
Contact Email: info@ventherm.dk

Contact Person: Allan Hansen

Visiting our website

When you visit our website, we use cookies to ensure it functions correctly. More details about our cookie policy can be found in our cookies policy.

Communication with potential customers

When you contact us via contact form, email, or phone to inquire about our services, we process the personal data you provide to respond to your questions and provide relevant information about our services. We typically process the following ordinary information: name, email, and phone number.

We have a legal basis for processing this information under GDPR Article 6(1)(f). We delete your communication with us as soon as it is clear whether you want our services or not. In special cases where retention is necessary, we will specify the reason for this.

Customers

To ensure the proper delivery of our services, we communicate with our customers and process information about them, such as name, address, services, special agreements, and payment information. The legal basis for processing this information is GDPR Article 6(1)(b). When the service is delivered and any outstanding issues are resolved, we promptly delete the personal data.

Accounting

We are obliged to retain accounting documents in accordance with the Accounting Act. This includes keeping invoices and similar documents, which may contain ordinary personal data such as name, address, and service description. The legal basis for processing personal data for accounting is GDPR Article 6(1)(c).

We retain this information for at least 5 years after the end of the relevant financial year.

Job applications

We receive and evaluate job applications for potential employment in our company. The legal basis for processing personal data in connection with job applications is GDPR Article 6(1)(f).

If you send an unsolicited application, we will evaluate the application and delete your information if there is no match. If you apply for an advertised job, your application will be deleted after the right candidate is hired.

If you participate in a recruitment process or are hired, you will receive separate information about how we process your personal data in this context.

Data processors

We work with external suppliers and data processors, including system providers, consultants, IT hosting, and marketing services. Data processors must comply with our standards for data protection and security to protect your personal data.

Disclosure of personal data

We do not disclose your personal data to third parties.

Profiling and automated decisions

We do not perform profiling or use automated decisions.

Transfers to third countries

We primarily use data processors within the EU/EEA or outside the EU/EEA who can offer adequate protection for your personal data. We always ensure that appropriate measures are in place to protect your personal data when transferred to third countries.

Data security

We implement appropriate technical and organizational measures to protect the processing of personal data. This includes risk assessments and continuous updating of our procedures and employee training on GDPR.

Data subjects' rights

You have certain rights under the GDPR regarding the processing of your personal data. If you wish to exercise your rights, please contact us.

Right of access: You have the right to access the information we process about you and additional information about the processing.

Right to rectification: You have the right to have incorrect information about yourself corrected.

Right to erasure: Under certain circumstances, you have the right to have information about you deleted before our usual deletion time.

Right to restriction of Processing: Under certain circumstances, you have the right to restrict the processing of your personal data.

Right to object: Under certain circumstances, you have the right to object to our otherwise lawful processing of your personal data, including for direct marketing.

Right to data portability: Under certain circumstances, you have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transfer this information from one data controller to another without hindrance.

You can read more about your rights in the Data Protection Agency's guide on the rights of data subjects, which can be found on the Data Protection Agency's website.

Withdrawal of consent

If our processing of your personal data is based on your consent, you have the right to withdraw your consent.

Complaint to the Data Protection Agency

If you are dissatisfied with our processing of your personal data, you have the right to lodge a complaint with the Data Protection Agency. You can find the Data Protection Agency's contact details on their website.

We encourage you to familiarize yourself with the GDPR to stay updated on the regulations. This privacy policy is part of our efforts to protect your personal data and ensure compliance with applicable data protection legislation.

Security breaches

To strengthen our commitment to data protection and comply with GDPR requirements, we have implemented clear security breach procedures. These steps are designed to handle situations where our data security may have been compromised.

A security breach can be anything from the loss of a laptop to unauthorized access to our data systems. It is important to understand that any loss, alteration, unauthorized access, or leakage of personal data is considered a security breach.

Steps for reporting security breaches:

Detection: Discovering a potential security breach.

Reporting: Immediate reporting to the data protection officer.

Investigation: Conducting a thorough investigation of the security breach.

Confirmation: Confirming whether it is a security breach.

Notification: If it is a serious breach, the affected parties and relevant authorities will be notified within 72 hours.

Roles:

Data protection officer: Responsible for coordinating response and notification.

IT security officer: Leads technical investigations and corrective measures.

Management level: Decision-making regarding response and resources.

Contingency plans: After the breach, contingency plans are evaluated and updated.

Improvements: Implementing improvements to prevent recurrence.

Changes to the privacy policy

We reserve the right to update this privacy policy from time to time to reflect changes in our practices or legal requirements. Changes will be published on our website along with the date of the last update.