Privacy Policy

Visar Systems AB | Version 1.0 | 26 November 2026

Policy owner: Simon Ekman, CEO | Contact: privacy@visar-systems.com

Approved by Simon Ekman, CEO, on 26 November 2026.

Who is responsible, and who does this policy cover?

Visar Systems AB, registration number 559528-7425, is the controller of the personal data we process for the business purposes described here. Contact privacy@visar-systems.com with privacy questions or requests to exercise your rights.

This policy covers website visitors, prospects and customer contacts, users of our account and documentation services, and job applicants, including the documented security interview conducted during recruitment. Employment and contractor relationships and the separate security-classification process are outside the scope of this policy and require separate privacy information.

Customer personal data that we process on a customer's behalf during support or other agreed services is governed by the applicable customer agreement and Data Processing Agreement (DPA), as explained below.

We never sell personal data, we do not authorise third parties to use personal data we hold to train AI models and we do not train AI models ourselves on personal data.

What personal data do we process, and why?

Business contacts and personal outreach

Personal data: names, employer, role, business email address, phone number and correspondence. We obtain these details from you, your organisation or public professional channels. We do not purchase contact lists.

Purpose and legal basis: our legitimate interests in answering enquiries, identifying relevant business opportunities and managing relationships with prospects, customers and partners. Outreach is personal and directed to relevant business contacts. We have no automated marketing campaigns.

Agreements, electronic signing and invoicing

Personal data: relevant business contact details and correspondence, personal data contained in agreement and invoicing records, and signer identification, authentication and signature evidence for the signing method used. Customer purchases are handled through agreements and invoices.

Purpose and legal basis: our legitimate interests in administering business agreements, identifying authorised representatives and keeping evidence of agreements; performance of a contract where you personally are a party; and legal obligations concerning accounting, tax and record keeping.

Accounts and customer documentation

Personal data: name, email address and IP address collected for the login service and customer wiki.

Purpose and legal basis: our legitimate interests in providing and protecting authorised access to our services and documentation, administering permissions and maintaining accountability. Where an account is necessary to perform a contract directly with you, that processing is based on performance of the contract.

Website operation and security

Personal data: IP address only.

Purpose and legal basis: operating and protecting our website and services, investigating faults and security incidents, and maintaining relevant technical records, based on our legitimate interest in providing reliable and secure services.

Our website does not use visitor analytics, advertising trackers or behavioural tracking. Cookies are limited to essential login and session-management functions.

Recruitment

Personal data: contact details, CVs, application letters, interview notes, documentation of the security interview and references, as relevant to the position.

Recruitment information held by Visar is stored on servers under our control. We may engage external recruitment providers to assist with recruitment and share only the application information necessary for that purpose. These providers will not be given access to Visar's internal systems or to security-interview answers or documentation.

Where an external recruitment provider is involved, applicants will be informed about its role and how their personal data is handled.

Purpose and legal basis: our legitimate interest in assessing applicants' suitability for the position, including relevant security requirements, and recruiting trustworthy people. A security interview is conducted and documented as part of recruitment. Information is limited to what is relevant to the position.

How do we handle customer data during support?

DeeDee does not send customer-environment data or telemetry to Visar by default. Customers operate their environments, and Visar has no routine access.

Our Terms of Service govern processing on a customer's behalf during support or other agreed services. Visar acts as processor, or as subprocessor where the customer is itself a processor.

Standard limited support involves customer-authorised, supervised screen viewing and verbal guidance. Broader processing requires the customer's documented instructions and agreement under the DPA.

We separately act as controller for our own business contacts, agreement administration, invoicing and legal obligations. If a request concerns personal data we process on a customer's behalf, we will direct it to the responsible customer and provide the assistance required by the DPA.

How do we use AI?

Where the information and its classification permit, we use AI systems to assist with drafting correspondence and general business administration.

We do not use personal data to train or fine-tune our internal AI models, and we do not authorise third parties to train models on personal data we hold.

Decisions about individuals are made by people. We do not make decisions with legal or similarly significant effects on individuals solely through automated processing.

Where is information stored, and who can receive it?

Our own systems and backups are hosted on Visar's own hardware in Sweden. Access by Visar approved personnel is from within the EU/EEA only.

We may share personal data with service providers supporting accounting, invoicing, agreement signing, recruitment and other business administration. These providers must meet applicable EU/EEA data protection requirements, including GDPR. Where providers process personal data on our behalf, we have a data processing agreement (DPA) in place and require them to follow our documented instructions.

The relevant providers' privacy policies also apply to their own processing. This policy continues to apply to Visar's processing.

Third-party services may involve processing outside the EU/EEA. Such transfers require applicable GDPR safeguards. Contact privacy@visar-systems.com for details of the relevant safeguards and how to obtain a copy.

We may also disclose information where necessary to meet a legal obligation or establish, exercise or defend legal claims.

How do we protect personal data?

Personal data on our self-hosted systems is encrypted in transit and at rest, including in backups. Access is restricted to authorised people who need it for their work. We apply protection appropriate to the information's classification and the risks involved.

We protect information according to its sensitivity and applicable contractual requirements. Customer instructions and the DPA govern customer personal data processed on a customer's behalf.

How long do we keep personal data?

Retention depends on the purpose and applicable obligations. We delete or anonymise personal data when it is no longer needed. The following periods and criteria apply to the relevant records, rather than a single retention period for everything.

Prospects and business correspondence

For prospects who do not become customers, we retain relevant contact details and correspondence for up to 24 months after the last meaningful contact, provided they remain necessary. An objection to direct marketing is honoured immediately; a minimal suppression record may be retained to respect it.

Customer contact details and relevant correspondence are retained during the business relationship and afterwards only while needed to administer remaining obligations, meet legal requirements or establish, exercise or defend claims within the applicable limitation periods.

Agreement and accounting records

Accounting information is retained through the end of the seventh year after the end of the calendar year in which the relevant financial year ended, as required by Swedish accounting law. Agreement and signing evidence may be retained longer where necessary for remaining contractual obligations or legal claims.

Recruitment records

We normally retain relevant application information for future vacancies for up to 24 months after the recruitment process ends, provided it remains relevant. We retain only information needed for that purpose and delete or anonymise it earlier if it is no longer relevant or you withdraw consent. You can withdraw consent at any time by emailing privacy@visar-systems.com.

Backups

A backup may temporarily contain information deleted from active systems until that snapshot expires through normal rotation. Backups are protected and access is restricted.

Customer personal data processed on a customer's behalf is returned or securely deleted at the customer's choice when the relevant processing services end, subject to the DPA and legally required retention.

Cookies and external website resources

We use only essential cookies for login and session management. We do not use analytics or advertising cookies.

External services and website resources are subject to the relevant provider's privacy information.

Links to other websites take you to services with their own privacy policies.

What are your rights?

Depending on the circumstances, you have the right to:

- Request access to your personal data and information about its processing.
- Request correction of inaccurate information and completion of relevant incomplete information.
- Request deletion or restriction of processing.
- Object to processing based on legitimate interests.
- Object to processing for direct marketing.
- Receive your data in a portable format where the legal conditions are met.
- Withdraw consent where processing relies on consent, without affecting earlier lawful processing.

Email privacy@visar-systems.com to exercise your rights. Requests are normally free of charge. A fee may be charged only in the limited circumstances permitted by GDPR. We may request the minimum information necessary to verify your identity.

We respond without undue delay and normally within one month. Where permitted because of a request's complexity or the number of requests, the period may be extended by up to two further months. We will explain an extension within the first month.

You may lodge a complaint directly with the Swedish Authority for Privacy Protection (IMY). You do not need to contact Visar first.

Providing information and changes to this policy

Providing personal data is generally voluntary. Some information is needed to answer an enquiry, administer an agreement, provide an account or assess an application. If the necessary information is not provided, we may be unable to carry out that activity.

We review this policy regularly and update it when our processing changes. The latest approved version will be published with its revision date. We will provide additional information about significant changes where required.