

Aureo Job Privacy Policy

Responsible entity: Aureo Technologies
Company / account: Aureo Technologies
Type: Política corporativa de Aureo Job
Jurisdiction: Estados Unidos
Version: 2.1
Effective date: 15/07/2026
Last updated: 19/07/2026
Document ID: privacy-v2.1-4730

Aureo Technologies

Version 2.1

Effective July 15, 2026

This Privacy Policy explains how Aureo Technologies collects, uses, retains, discloses, and protects personal information related to Aureo Job, our websites, demo requests, free trials, company accounts, communications, and support services.

Aureo Job is a B2B SaaS platform for field service companies. This Policy should be read together with the Aureo Job Terms of Service and, where applicable, the applicable Data Processing Agreement (“DPA”).

1. Scope of this Policy

This Policy applies to the personal information that Aureo collects directly from:

- Visitors to Aureo Job websites.
- Individuals who request a demo, commercial information, or a free trial.
- Representatives, owners, administrators, and business contacts of customer companies.
- Authorized Users who access or use Aureo Job.
- Individuals who communicate with Aureo by email, technical support, forms, calls, or enabled channels.
- Technical, security, and usage information related to platform access.

This Policy also explains, in general terms, how Aureo processes information uploaded by customer companies inside Aureo Job.

It does not replace the privacy notices, employment notices, geolocation policies, video surveillance notices, attendance policies, or communications that each Customer Company must provide to its own workers, contractors, end customers, or third parties.

2. Privacy roles

Aureo may play different roles depending on the information involved.

2.1 Information from a direct relationship with Aureo

For information about visitors, prospects, account administrators, business contacts, billing, support, Aureo communications, and platform security, Aureo normally acts as the responsible party, business, or controller of that information, depending on the applicable law.

2.2 Data uploaded by a Customer Company

For information that a Customer Company enters, generates, records, or manages inside Aureo Job about its workers, contractors, end customers, properties, work orders, photos, attendance, location, invoices, estimates, communications, or operational activities ("Customer Data"), the Customer Company normally determines the purposes and means of processing.

In those cases, the Customer Company acts as the responsible party, business, or controller, and Aureo acts as a service provider, processor, or equivalent role, as applicable.

Aureo processes Customer Data only to provide, protect, maintain, and improve the Service, in accordance with the documented instructions of the Customer Company, the Terms of Service, the applicable DPA, and the law.

If you are a worker, end customer, contractor, or user of a Customer Company and wish to exercise rights related to Customer Data, you must first contact that Customer Company. Aureo may reasonably assist the Customer Company when necessary and permitted.

3. Information we may collect

3.1 Information provided directly

We may collect information that you provide when creating an account, requesting a demo, starting a trial, purchasing a subscription, communicating with us, or using features of the Service, including:

First name, last name, email address, phone number, and job title.

Company name, business type, number of workers, business address, and operating area.

Username, encrypted password, language preferences, and account settings.

Billing information, payment history, subscription, invoices, and related communications.

Messages, support requests, feedback, questions, suggestions, and files sent to Aureo.

Information that you provide in forms, surveys, events, demos, or commercial communications.

3.2 Data processed on behalf of Customer Companies

Aureo Job may process, on the instructions of a Customer Company, categories of Customer Data such as:

Contact details of end customers, prospects, workers, contractors, and users.

Addresses, properties, service locations, and operational references.

Estimates, proposals, work orders, recurring jobs, invoices, payments, expenses, and reports.

Schedules, attendance, clock-ins and clock-outs, time history, assignments, crews, and permissions.

Before-and-after photos, work evidence, signatures, notes, documents, and attachments.

Inventory, materials, equipment, maintenance, costs, and job profitability data.

Audit logs, activity within the Account, administrative actions, and relevant changes.

Operational communications sent or recorded by the Customer Company through the Service.

3.3 Technical and usage information

When you use our sites or the Service, we may automatically collect information such as:

IP address.

Browser type, device, operating system, language, and regional settings.

Session identifiers, access date and time, and pages or features used.

Technical logs, security events, errors, diagnostics, and Account-related activity.

Approximate information derived from IP address, when available.

Cookies, local storage, and similar technologies necessary for authentication, security, preferences, or operation of the Service.

3.4 Location, attendance, and photo evidence

When a Customer Company enables time clock, GPS, operational tracking, routes, dispatch, photos, or evidence features, Aureo Job may process:

Approximate or precise device location.

Date, time, and coordinates associated with a clock-in, clock-out, visit, job, route, or operational event.

Evidence photos, attendance photos, or documents linked to the operation.

Information related to an authorized work session or tracking event.

Location collection depends on the user granting permissions on their device or browser and on the Customer Company enabling the corresponding feature.

As of the effective date of this Policy, Aureo Job active tracking features are designed to operate during time clock actions or authorized foreground work sessions. They are not designed to collect continuous location when the browser is closed or locked.

Aureo does not use photos of workers or customers for facial recognition or to create biometric identifiers.

The Customer Company is responsible for providing clear notices and obtaining consents, authorizations, or legal bases when necessary for GPS, photos, attendance, signatures, communications, activity monitoring, or any other personal information of workers or third parties.

3.5 Payment information

Payments are processed through Stripe or another authorized processor. Aureo does not store full credit or debit card numbers in its ordinary systems.

We may receive limited transaction information, such as payment status, amount, date, partially masked payment method, transaction identifiers, invoices, refunds, disputes, or failed payments.

3.6 Third-party information

We may receive information from authorized vendors, integrations enabled by the Customer, payment processors, authentication providers, maps, messaging, support, analytics, security, or infrastructure providers, only to the extent necessary to provide or protect the Service.

4. How we use information

We may use personal information to:

Create, administer, and protect Aureo Job Accounts.

Provide, operate, maintain, update, and improve the Service.

Authenticate users, enforce permissions, and prevent unauthorized access.

Process subscriptions, payments, invoices, renewals, cancellations, and related requests.

Respond to demo, technical support, privacy, security, or legal requests.

Facilitate features requested by the Customer Company, including scheduling, crews, attendance, GPS, photos, billing, reports, and automations.

Detect, investigate, prevent, and respond to fraud, abuse, errors, failures, unauthorized access, or security incidents.

Generate reports, aggregated statistics, or de-identified information for operation, security, analysis, and improvement of the Service.

Comply with legal, tax, regulatory, contractual, or audit obligations.

Send administrative, technical, security, billing, product, or legal change communications.

Send commercial communications when there is consent, a prior business relationship, or another basis permitted by law. You may unsubscribe from promotional communications through the link included in the message or by writing to privacy@aureotechnologies.com.

Protect the rights, property, security, and continuity of Aureo, its customers, users, and third parties.

Aureo Job may offer operational suggestions, automations, assignments, reports, or recommendations. These tools do not make employment, legal, tax, credit, or hiring decisions exclusively by automated means with legal or similarly significant effects for a person. The Customer Company keeps final decision-making authority over its operation.

5. How we share information

Aureo may share personal information only when necessary and in accordance with this Policy, the Terms of Service, the applicable DPA, Customer Company instructions, or the law.

We may share information with:

5.1 The Customer Company and its Authorized Users

Customer Data may be visible to administrators, supervisors, crew leaders, administrative personnel, workers, or other Authorized Users according to the permissions configured by the Customer Company.

5.2 Vendors and subprocessors

We may use vendors that help us operate the Service, including providers of:

Hosting, infrastructure, storage, databases, and backups.

Payment processing.

Email, notifications, messaging, and support.

Maps, geocoding, location, or routes.

Monitoring, technical logs, error detection, and security.

Administration tools, operational analytics, and Service continuity.

These providers may process information only according to our instructions, their contractual obligations, and applicable law.

The current list of subprocessors may be requested by writing to privacy@aureotechnologies.com.

5.3 Integrations enabled by the Customer

When a Customer Company enables an integration, Aureo may exchange the information strictly necessary to enable it, according to the Customer's configuration and instructions.

5.4 Legal requirements and protection of rights

We may disclose information when we reasonably believe it is necessary to comply with a law, government request, subpoena, court order, fraud investigation, protection of rights, safety, prevention of harm, or enforcement of our agreements.

5.5 Corporate transactions

We may share information in connection with a merger, acquisition, financing, corporate reorganization, sale of assets, or business transfer. In those cases, we will seek to ensure that the information continues to be protected under this Policy or a substantially equivalent policy.

6. No sale or behavioral advertising

Aureo does not sell personal information as a business model.

Aureo does not share personal information for cross-context behavioral advertising or to create advertising profiles of users, workers, end customers, or visitors.

Aureo does not use Customer Data to train third-party general-purpose artificial intelligence models without the express authorization of the Customer Company.

If these practices change in the future, Aureo will update this Policy, implement the required choice mechanisms, and honor applicable opt-out signals in accordance with the law.

7. Cookies, local storage, and similar technologies

Aureo uses cookies, local storage, and similar technologies to:

Maintain authenticated sessions.

Remember language, preferences, and settings.

Protect against fraud, unauthorized access, and misuse.

Maintain the stability, security, and operation of the Service.

Understand, in aggregate form, the performance and technical use of our sites or features.

You can configure your browser to block or delete cookies. However, certain features, including login, security, language, or preferences, may stop working correctly.

When Aureo implements non-essential cookies or technologies that require consent under applicable law, it will request that consent before activating them.

8. Retention of information

We retain personal information for as long as reasonably necessary to fulfill the purposes described in this Policy, provide the Service, maintain security, resolve disputes, enforce our agreements, and comply with legal, tax, accounting, or audit obligations.

In general:

Account information is retained during the subscription term and in accordance with applicable billing, security, and compliance obligations.

Customer Data may remain available for up to thirty (30) calendar days after cancellation or termination to allow a reasonable export, unless restricted by security, fraud, serious breach, or legal obligation.

Temporary report, CSV, XLSX, and PDF files may be deleted after fourteen (14) days.

Export packages for privacy requests may be deleted after seven (7) days.

Temporary compliance documents may be deleted after thirty (30) days.

Technical logs, asynchronous job metadata, and audit logs may be retained for at least ninety (90) days, or longer when necessary for security, support, compliance, dispute, or fraud prevention.

Raw GPS data may be retained for up to thirty (30) days; related session summaries or audit records may be retained for ninety (90) days or longer when there is an operational, contractual, or legal need.

Residual copies may remain temporarily in protected backups until deletion according to ordinary backup and recovery cycles.

9. Security

Aureo applies commercially reasonable administrative, technical, and organizational measures to protect personal information against unauthorized access, loss, alteration, destruction, or improper disclosure.

These measures may include access controls, role-based permissions, logical separation between customer companies, audit logs, security validations, session protection, backups, monitoring, and incident response procedures.

However, no internet-connected system is completely secure. We cannot guarantee absolute security, uninterrupted availability, or total absence of errors.

If Aureo confirms a security incident that materially compromises Customer Data under our control, we will notify the Customer Company without undue delay and provide reasonably available information to support its applicable legal obligations.

10. Your privacy rights

Depending on your jurisdiction and relationship with Aureo, you may have the right to request:

Confirmation of whether we process your personal information.

Access to personal information and categories of information processed.

Correction of inaccurate information.

Deletion of personal information, subject to legal exceptions.

Portability of certain information.

Information about purposes, categories of recipients, and sources of information.

Limitation of use or disclosure of sensitive personal information, when applicable.

Opt out of sale or cross-context behavioral advertising, when applicable.

No discriminatory treatment for exercising privacy rights.

Appeal of a decision related to a privacy request, when applicable law recognizes that right.

To exercise a right related to information that Aureo controls directly, write to privacy@aureotechnologies.com with the subject "Privacy Request".

We may request reasonable information to verify your identity, authority, or relationship with the Account before processing the request. You may also designate an authorized agent when applicable law permits; we may request proof of authorization and identity.

We will respond according to the timeframes required by applicable law. When a request cannot be completed in whole or in part, we will explain the reason when required by law.

If you disagree with a decision about your request and applicable law recognizes a right to appeal, you may send an appeal to privacy@aureotechnologies.com with the subject "Privacy Appeal".

Data controlled by a Customer Company

If your request relates to workers, end customers, work orders, attendance, photos, GPS, invoices, communications, or any other Customer Data, you must direct it first to the corresponding Customer Company.

Aureo may forward your request to the Customer Company or cooperate with it to address the request according to its instructions and legal obligations.

11. Sensitive personal information

Aureo Job may process information considered sensitive under some laws, such as precise location, photos, operational documents, attendance data, or information associated with an employment relationship.

Aureo uses and discloses that information only as necessary to:

Provide the Service requested by the Customer Company.

Maintain, secure, and protect the Account and platform.

Detect, prevent, and investigate fraud, incidents, or illegal activity.

Comply with legal, contractual, or audit obligations.

Process features specifically enabled by the Customer Company.

Not infer personal characteristics about a person.

When the law requires it, individuals may request to limit the use or disclosure of sensitive information by contacting privacy@aureotechnologies.com. Requests related to Customer Data should primarily be directed to the responsible Customer Company.

12. International transfers

Aureo Job is primarily intended for companies operating in the United States. Personal information may be processed in the United States and in other places where Aureo or its authorized providers operate.

When applicable law requires specific mechanisms for international transfers, Aureo will adopt reasonable measures and appropriate contracts to protect the information in accordance with that law.

13. Minors

Aureo Job is not directed to children under 13 years of age, and we do not knowingly collect personal information from children under 13.

If you believe that a child under 13 provided personal information to Aureo without appropriate authorization, write to privacy@aureotechnologies.com so that we can review and take reasonable action.

14. Regulated information and unauthorized uses

Unless Aureo expressly agrees otherwise in writing, Aureo Job is not designed to receive, store, or process:

Protected health information subject to HIPAA.

Full payment card information.

Social Security numbers, driver's licenses, passports, or other sensitive government identifiers.

Biometric information used for identification.

Information regulated by special laws that requires additional agreements.

Customer Companies must not upload such information without written authorization from Aureo and without the corresponding legal, technical, and security agreements.

15. Third-party sites and services

The Service may contain links, integrations, or references to third-party services. This Policy does not apply to the privacy practices of independent third parties.

We recommend reviewing the privacy policies of Stripe, map providers, integrations, communication tools, or other services that you use independently.

16. Google Workspace API data

When an authorized Company administrator connects a Gmail mailbox to Aureo Job, the Company gives Aureo Job access only to the minimum Google data and permission needed for the business email feature.

Data accessed and stored

Aureo Job receives the Google Account identifier and email address for the mailbox selected by the user. It receives OAuth access and refresh tokens and stores those tokens encrypted. It also processes the recipients, subject, message body, and attachments that an authorized user instructs Aureo Job to send through that mailbox. Aureo Job may retain limited outgoing-message metadata, such as sender, recipient, subject, provider message identifier, time, and delivery status, for visible history, security, support, and audit purposes.

How the data is used

Aureo Job uses the Google Account identity to display and enforce the authorized sender and uses the `https://www.googleapis.com/auth/gmail.send` permission solely to send estimates, invoices, reminders, notices, and other messages requested through the Company's user-facing workflows. Aureo Job does not request permission to read, modify, or delete the Gmail inbox and does not read mailbox contents.

Sharing and prohibited uses

Google user data is not sold, used for advertising, transferred to data brokers, used to determine creditworthiness or for lending, or used to create, train, or improve generalized artificial intelligence or machine-learning models. It is disclosed only to Google to perform the requested send operation, to service providers when strictly necessary to operate or secure the user-facing feature under appropriate obligations, for security purposes, or when required by law. Human access is prohibited except with the user's affirmative authorization for specific support, when necessary for security, or when required by law.

Retention, protection, and deletion

OAuth tokens are encrypted at rest, access is restricted by Company and role, and security-relevant actions are audited. Disconnecting Gmail from Aureo Job removes the active stored tokens and stops future Gmail API access. A user may also revoke access from the Google Account security settings or request deletion through privacy@aureotechnologies.com, subject to limited security, audit, and legal retention obligations described in this Policy.

Aureo Job's use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

17. Changes to this Policy

We may update this Policy to reflect legal, technical, commercial, operational, security, or functional changes.

The updated version will indicate its effective date and version number. When a change is material, we will seek to notify you by email, within the Service, or through a visible notice before it takes effect, when reasonably possible.

Continued use of Aureo Job after the effective date of an updated Policy will be subject to the current version, unless applicable law requires another form of consent.