GRAVUN PRIVACY POLICY

Effective Date: September 22, 2026

Gravun Inc. (**"Gravun," "we," "us,"** or **"our"**) provides business software for managing customer relationships, service work, communications, payments, and electronic signatures.

This Privacy Policy explains how we handle personal information through www.gravun.com, app.gravun.com, our support and business communications, and the customer-facing pages and features operated through our platform.

Personal information means information about an identified or identifiable individual, including information treated as personal data or personal information under applicable law.

1. Whose Information This Policy Covers

1.1 Website Visitors and Business Contacts. This Policy covers information we collect when you visit our website, request information, communicate with us, or otherwise interact with Gravun.

1.2 Workspace Users. It also covers individuals who create, administer, or use a workspace for a business subscribing to Gravun (**"Customer"**).

1.3 Customers' Clients and Other Individuals. You may interact with Gravun without opening an account, for example, when you book a service, receive an estimate, sign a document, pay an invoice, exchange messages, or speak with a Customer's AI receptionist. We refer to individuals interacting with our Customers in this way as **"End Clients."**

1.4 Different Responsibilities. Gravun determines how information is handled for its own account administration, billing, security, support, and business communications. When a Customer uses Gravun to manage its clients, staff, documents, or communications, we generally process that information on the Customer's behalf and according to its instructions. Depending on applicable law, these roles may be described as a controller or business, and a processor or service provider.

1.5 Customer Privacy Practices. A Customer is responsible for explaining its own collection and use of personal information, including why it contacts you, records a call, requests a signature, or retains a business record. This Policy describes Gravun's handling of that information; it does not replace the Customer's privacy notice.

1.6 Additional Notices. Specific features may display additional notices, including electronic-signature consent, call-recording notices, AI disclosures, or cookie choices. These explain the particular activity when it occurs. This Policy does not itself obtain consent for every activity described below.

2. Information We Collect

2.1 Account and Business Information. We collect information supplied to establish and administer a workspace, including names, business names, contact details, account identifiers, roles, authentication information, subscription selections, and account preferences.

2.2 Billing Information. We receive subscription and transaction information such as billing contacts, billing addresses, payment status, invoice details, transaction references, and limited payment-method information. Payment processors collect payment credentials through their payment interfaces. Gravun does not require you to send full card details through support messages or ordinary workspace fields.

2.3 Information Held in Customer Workspaces. Depending on the features a Customer uses, its workspace may contain:

Category	Examples
Contact and client records	Names, email addresses, telephone numbers, service addresses, contact preferences, and business relationships
Service and transaction records	Enquiries, appointments, estimates, invoices, work orders, change orders, job notes, and payment status
Communications	Emails, text messages, attachments, delivery records, call details, recordings, transcripts, and summaries
Signing records	Documents, names, signatures, entered field values, consent records, timestamps, and technical signing evidence
Uploaded or	Files, photographs, contact lists, historical records,

Category	Examples
imported materials	and information imported from connected systems
Consent and preference records	Subscription choices, communication permissions, opt-outs, suppression records, and associated evidence

Information in these categories may concern End Clients, Customer personnel, suppliers, or other people identified in Customer materials.

2.4 Device, Usage, and Security Information. We collect technical information associated with use of our websites and Service, such as IP addresses, browser and device details, timestamps, session identifiers, pages or features accessed, application events, error information, and security logs. An IP address may indicate an approximate location; it does not establish a person's identity or precise physical location.

2.5 Support Information. We collect information you provide when seeking assistance, including correspondence, issue descriptions, and files or screenshots you choose to share. Please avoid sending information unrelated to the support request.

2.6 Connected-Service Information. If a Customer or user connects another service, we receive the information authorized through that connection. Depending on the integration, this may include mailbox content, calendar events, contact records, imported CRM records, or information needed to perform an authorized action.

2.7 Sensitive Information. Communications and documents may contain financial, private, or otherwise sensitive information depending on what Customers and individuals submit. The platform is not an invitation to upload unnecessary identity documents, payment credentials, medical records, or other sensitive information. Customers must assess whether a proposed use is appropriate and permitted under their agreement with Gravun.

3. Where Information Comes From

3.1 Directly from You. We receive information when you register, complete a form, communicate with us, interact with a Customer through the platform, or submit information during a transaction.

3.2 From Customers and Their Users. Customers may enter information about you, import existing records, invite you to use a feature, or send you a document.

3.3 From Connected Providers. Authorized integrations, payment processors, communication providers, and authentication services supply information needed to operate the selected features and report their results.

3.4 Automatically. Our systems and service providers generate technical, delivery, usage, and security information when the websites or Service are used.

4. How We Use Information

4.1 Providing the Service. We use information to establish accounts, authenticate users, apply permissions, store records, operate selected features, process Customer instructions, and deliver the requested service.

4.2 Customer Workflows. On a Customer's behalf, we process information to support scheduling, estimating, invoicing, communications, electronic signing, reporting, and authorized automation.

4.3 Billing and Administration. We use relevant information to administer subscriptions, process charges, reconcile payments, maintain business records, and communicate about accounts.

4.4 Support and Reliability. We use information reasonably necessary to answer requests, investigate errors, maintain compatibility, and assess service performance. Access to Customer records for these purposes remains subject to applicable permissions, contractual restrictions, and law.

4.5 Security and Abuse Prevention. We use relevant records to protect accounts, investigate suspicious activity, prevent fraud or misuse, enforce appropriate restrictions, and respond to security incidents.

4.6 Business Communications. We use contact information to respond to enquiries and provide service announcements. Where permitted by law and subject to required consent, we may also send information about Gravun's products and services. Marketing choices are explained in Section 12.

4.7 Legal and Regulatory Matters. We may process information to comply with legal obligations, respond to valid legal requests, preserve relevant evidence, and establish, exercise, or defend legal claims.

4.8 Product Evaluation. We may use service-performance information and lawfully aggregated or de-identified information to understand how features operate and improve the Service. This does not authorize unrestricted use of Customer document, message, or recording content for unrelated product development.

4.9 Purpose Limitations. We do not treat the availability of information in a workspace as permission to use it for any purpose. A materially different use requiring consent will be explained and authorized before it begins.

5. Gravun Sign

5.1 Signing Information. When a document is sent through Gravun Sign, we process the document, sender and signer contact information, completed fields, typed or drawn signatures, and associated signing events.

5.2 Consent and Technical Evidence. Signing records may include the consent wording presented, its version and digital fingerprint, the recorded agreement, timestamps, IP address, browser or device information, signature method, and document fingerprints. A digital fingerprint is a technical value used to help detect changes to particular data.

5.3 Completed Documents and Certificates. The completed document and accompanying certificate contain information about the signing process. Copies are made available to the sender and sent to the signers involved in the transaction. Information included in the certificate, such as signing times and technical evidence, may therefore be visible to those recipients.

5.4 Signing Links. A person who obtains a signing link may be able to access the associated signing process, subject to the controls available for that transaction. Links should not be forwarded or shared with an unauthorized person.

5.5 Retention and Requests. Signing evidence may be needed to document consent, establish a transaction, or address a dispute. A request to erase personal information does not automatically require destruction of every executed document or related record. We assess requests according to our role, the Customer's lawful instructions, and applicable retention requirements and exceptions.

5.6 Copies Outside Gravun. Deletion from Gravun does not delete copies already held by the sender, other signers, or their advisers. Requests concerning those copies must be addressed to the relevant holder.

6. Calls, Messages, and AI Features

6.1 Communications Processing. Where enabled by a Customer, we process telephone numbers, email addresses, message content, call details, delivery events, and communication preferences to provide calling, messaging, and related functions.

6.2 Recordings and Transcripts. A Customer may enable call recording, transcription, or summarization. The resulting information is made available within that Customer's workspace according to its permissions. Recording and transcription require the notices and permissions applicable to the particular communication.

6.3 AI Receptionist and Assistant. AI features may process prompts, conversation content, recordings, transcripts, and relevant workspace information to answer enquiries, prepare summaries, draft content, or perform authorized actions.

6.4 Provider Processing. The information required for an enabled AI feature may be transmitted to the relevant model, voice, or transcription provider. The information involved depends on the feature and its configuration; enabling one feature does not mean every workspace record is sent to every provider.

6.5 Model Training. We do not use Customer Content, or authorize our subprocessors to use it, to train general-purpose AI models without separate affirmative authorization from the Customer and any additional permission required by law or the source of the information. Enabling an AI feature does not constitute that authorization. Restrictions applying to connected-service data continue to apply even where a Customer requests a broader use.

6.6 Review and Decisions. AI-generated information may be inaccurate. Customers determine how they use outputs and configure available approval controls. Where applicable law requires information about an automated decision or an opportunity for review, requests may be submitted to the Customer responsible for that decision or to us using Section 13.

7. Connected Accounts and Integrations

7.1 Authorized Access. Connections to services such as Google, Microsoft, or a CRM operate using the permissions granted through the relevant authorization process. We use connected information to provide the functions selected by the Customer or user.

7.2 Mail and Calendar Connections. Depending on the permissions granted, mailbox and calendar features may access message content, attachments, recipients, event details, and related identifiers to display information, synchronize records, or carry out authorized communications and scheduling.

7.3 Google Data. Gravun's use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including its Limited Use requirements where applicable. We do not use that information for advertising or general-purpose model training. Human access is restricted to circumstances permitted by those requirements.

7.4 Revoking Access. You may revoke a connection through the relevant provider's account settings and, where available, within Gravun. Revocation stops further access through that authorization but does not necessarily delete information previously imported or lawfully retained. You may request deletion through the process in Section 13.

7.5 Customer-Selected Tools. If a Customer authorizes an external tool or AI connection to access its workspace, information supplied to that tool is also subject to the recipient's privacy practices. The Customer controls the permissions it grants and should review the recipient's terms before enabling access.

8. Who Receives Information

8.1 Customer Personnel. Information processed for a Customer is accessible to its authorized personnel according to workspace roles and permissions. A business administrator may manage accounts and access business records associated with its workspace.

8.2 Transaction Recipients. We disclose information to the recipients involved in a Customer-authorized workflow, such as a message recipient, document signer, invoice payer, or connected service receiving an instruction.

8.3 Service Providers. We engage providers for hosting, database storage, authentication, payment processing, communications, transcription, AI functionality, error monitoring, and support infrastructure. Depending on the feature, these include Supabase, Stripe, Twilio, Vapi, Deepgram, Anthropic, OpenAI, Resend, Postmark, Google Maps, and Sentry. Our marketing website also uses website-hosting services.

Providers receive the information necessary for their role, subject to applicable contractual and legal restrictions. Some providers, including payment processors, may also process certain information for their own legal, fraud-prevention, or regulated purposes.

8.4 Provider Information. Details about the providers processing Customer information on our behalf are available through Subprocessor Schedule or by contacting our Privacy Officer. Customer-selected integrations are distinguished from Gravun's subprocessors in the applicable contractual documentation.

8.5 Advisers and Authorities. We may disclose relevant information to professional advisers or competent authorities where reasonably necessary and permitted by law, including to respond to valid legal process or protect legal rights. A request alone does not automatically justify disclosure of all information requested.

8.6 Business Transactions. Information may be disclosed in connection with a proposed or completed financing, reorganization, merger, or sale, subject to applicable legal requirements, appropriate confidentiality restrictions, and limitations on use. Where additional notice or consent is required, we will provide or obtain it.

8.7 No Unrestricted Disclosure Right. The categories above do not authorize disclosure contrary to the DPA, applicable law, or restrictions imposed by the source of the information.

9. Cookies and Similar Technologies

9.1 Application Technologies. The application uses technologies needed for authentication, session management, security, and preferences. Technical monitoring also supports error detection and reliability. Our application does not currently use third-party advertising cookies.

9.2 Website Technologies. The marketing website has a separate technical configuration. The Cookie Notice at www.gravun.com identifies the technologies used there, their purposes, and available choices. Where required, optional technologies are subject to consent before activation.

9.3 Communication Tracking. Messages and links may generate delivery, opening, or click information where the relevant feature and provider support it. These records may be made available to the Customer sending the communication. Their availability and accuracy depend on recipient software and privacy settings.

9.4 Choices. Browser settings and available consent controls can be used to manage cookies. Blocking technologies required for authentication or security may prevent parts of the Service from functioning. Browser cookie settings do not necessarily disable server-side records or message-delivery tracking.

9.5 Advertising Disclosures. Any activity constituting a sale of personal information, sharing for cross-context behavioural advertising, or targeted advertising under applicable law must be specifically disclosed with the required choices. Necessary service-provider disclosures are not treated as permission to introduce such activity.

10. International Processing

10.1 Primary Hosting. Gravun's core application database and storage are hosted in Canada. Certain providers, integrations, support activities, or communication routes may process information in the United States or other countries.

10.2 Foreign Access. Information processed outside your province, state, or country may be subject to the laws of that location and lawful access by its courts or public authorities.

10.3 Transfer Safeguards. We use contractual and other measures required by applicable law to address information transferred for processing. Where a privacy assessment or additional transfer arrangement is required, it must be completed before the affected transfer.

10.4 Further Information. You may contact our Privacy Officer for information about relevant cross-border processing and the safeguards applicable to your information. A Canadian primary hosting location does not mean that all processing takes place exclusively in Canada.

11. Retention and Security

11.1 Retention Criteria. We retain personal information for the period reasonably necessary for the purpose for which it was collected, subject to applicable law. Relevant considerations include the service relationship, Customer instructions, the nature of the record, accounting obligations, consent evidence, security needs, limitation periods, and actual or reasonably anticipated disputes.

11.2 Different Record Categories. Account records, billing records, communications, recordings, signed documents, and security logs may have different retention periods. We do not apply a single indefinite retention period to all personal information.

11.3 Customer Information. Information processed on behalf of a Customer is returned, deleted, or retained according to the applicable service agreement, DPA, lawful instructions, and legal requirements. Workspace closure does not necessarily require immediate deletion of every related record.

11.4 Backups and Restricted Records. Information removed from active systems may remain in protected backups until the applicable backup cycle expires. Information retained for legal or security purposes remains subject to appropriate access and use restrictions. If a backup is restored, applicable deletion instructions must be reapplied.

11.5 Signing and Suppression Records. Deleting a contact profile does not necessarily delete executed documents or certificates containing that person's information. We may also retain limited suppression information to ensure an opt-out continues to be respected. Retention must remain justified for the particular record and purpose.

11.6 Safeguards. We apply administrative, technical, and organizational safeguards appropriate to the information and risks involved. No internet-based service can guarantee absolute security.

11.7 Security Concerns. Suspected unauthorized access or disclosure should be reported promptly to Hello@gravun.com. We assess incidents and provide notifications to affected Customers, individuals, or authorities where required by law and our applicable contractual obligations.

12. Your Choices

12.1 Account Details. Workspace users may update information available through their account settings or request assistance from their administrator.

12.2 Gravun Marketing. You may unsubscribe from Gravun marketing emails using the link provided or by contacting us. We may continue to send essential account, billing, security, or legal notices.

12.3 Customer Communications. To stop a Customer's marketing, use the unsubscribe or other opt-out method in its communication or contact that Customer. Where supported and stated in a text message, you may reply with the indicated opt-out keyword.

12.4 Consent Withdrawal. Where processing depends on consent, you may withdraw it subject to applicable legal restrictions. We will explain material consequences where relevant. Withdrawal generally affects future processing and does not retrospectively invalidate lawful processing already undertaken.

12.5 Optional Features. You may decline optional permissions or revoke integrations, although the associated feature may then be unavailable. We do not make unrelated optional processing a condition of providing a service where prohibited by law.

13. Privacy Requests and Complaints

13.1 Available Rights. Depending on your location, the applicable law, and our role, you may have rights to obtain information about processing, access personal information, correct inaccuracies, request deletion, receive a portable copy, withdraw consent, or object to or restrict specified processing.

13.2 Contacting Us. Submit a request to the Privacy Officer identified in Section 17. Describe the request and provide sufficient information to locate the relevant account, Customer, or interaction. Do not send government identification or other sensitive documents unless we specifically request an appropriate verification method.

13.3 Verification. We may take proportionate steps to verify identity and authority before disclosing or changing information. We use verification information for that purpose and related security or legal requirements.

13.4 Customer-Controlled Records. If the request concerns information we process for a Customer, we will identify or refer you to the responsible Customer where appropriate and assist it as required. We do not automatically override a Customer's lawful control of its records, and we remain responsible for any obligation the law places directly on Gravun.

13.5 Responses and Exceptions. We respond within applicable legal periods. If an extension, charge, or refusal is legally permitted, we will provide the required explanation. Access may be limited where necessary to protect another person's information, privileged material, security, or another legally protected interest.

13.6 Authorized Representatives. Where permitted by law, an authorized representative may submit a request. We may require evidence of authorization and appropriate identity verification.

13.7 Complaints and Appeals. If you disagree with our response, contact the Privacy Officer and ask for review or, where applicable, appeal. We will explain the outcome and available further steps as required by law. You may also complain to the privacy regulator or other authority with jurisdiction over the matter.

13.8 No Unlawful Retaliation. We will not discriminate or retaliate against you for exercising a protected privacy right. A feature may nevertheless become unavailable where it cannot operate without information you have lawfully declined to provide.

14. Additional Information for Canadian Residents

14.1 Accountability. Our Privacy Officer oversees Gravun's privacy practices and the handling of privacy enquiries and complaints.

14.2 Access and Correction. Subject to applicable exceptions, you may request access to information under our control and challenge its accuracy or completeness. Where a disagreement cannot be resolved, we will handle a request to record that disagreement as required by law.

14.3 Québec Residents. Where Québec law applies, your rights may include receiving eligible computerized information in a structured, commonly used technological format and requesting information about a decision based exclusively on automated processing. Applicable rights to submit observations for review, withdraw consent, or request cessation of dissemination or de-indexing are subject to the conditions established by law.

14.4 Processing Outside Québec. Personal information may be processed outside Québec as described in Section 10, subject to applicable assessment, contractual, and protection requirements.

14.5 Regulatory Complaints. Depending on the matter, you may contact the Office of the Privacy Commissioner of Canada or the applicable provincial privacy regulator, including the Commission d'accès à l'information du Québec.

15. Additional Information for United States Residents

15.1 Applicability. State privacy rights depend on the law of your state, whether it applies to the relevant activity, and whether Gravun acts as a business or controller, or processes information for a Customer. This section does not imply that every state privacy statute applies to Gravun.

15.2 Categories and Purposes. The categories described in Section 2 include identifiers, account and commercial information, internet or network activity, approximate location derived from technical information, audio and electronic records, and professional information. Documents or communications may also contain information classified as sensitive under applicable law. Sections 3, 4, and 8 explain the sources, purposes, and recipient categories; Section 11 explains retention criteria.

15.3 State Rights. Where applicable, rights may include access, correction, deletion, portability, and opting out of sale, targeted advertising, or specified profiling. Some laws also provide rights concerning sensitive information or information about third-party disclosures.

15.4 Requests and Appeals. Requests may be submitted under Section 13. Where state law provides an appeal right, reply to our decision or contact the Privacy Officer with the subject "Privacy Appeal." We will respond and provide information about further complaint options within the applicable period.

15.5 Browser Signals. Where legally required for an applicable processing activity, we recognize qualifying browser-based opt-out preference signals. Their effect depends on the browser, device, and information we can reasonably associate with the signal.

15.6 California Notices. Where the California Consumer Privacy Act applies to information for which Gravun acts as a business, applicable notices at collection and any required sale, sharing, or sensitive-information choices will be provided at or before collection. Where Gravun acts as a service provider or contractor for a Customer, requests concerning that Customer's information will be handled in accordance with Section 13.4.

16. Children and Policy Changes

16.1 Children. Gravun's workspace service is intended for business use and is not directed to children. If you believe a child has provided information through the Service in circumstances requiring parental authorization, contact our Privacy Officer so that we can investigate and take appropriate action with the responsible Customer.

16.2 Updates. We may revise this Policy to reflect changes in our services, practices, or legal obligations. The updated version will show its effective date. We will provide additional notice of material changes where appropriate or required.

16.3 New Uses. Updating this Policy does not by itself authorize a new use of personal information requiring consent. We will obtain any additional consent required before beginning that use.

17. Contact the Privacy Officer

For privacy questions, requests, complaints, or information about our providers and international processing, contact:

Privacy Officer Gravun Inc.
Name: Ahmed Radi
Title: Founder
Email: Hello@gravun.com
Postal address: 10 Four Seasons Place, Etobicoke, ON M9B 6H7